UNIVERSIDAD DE SOTAVENTO

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL
AUTONOMA DE MEXICO

FACULTAD DE INFORMATICA

"FIREWALL COMO CONTROL DE SEGURIDAD EN LA UNIVERSIDAD DE SOTAVENTO"

ESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN INFORMATICA

PRESENTA:
DENNIS NORELY LUIS SANTIAGO

ASESOR DE TESIS:
LIC. RAUL OCAMPO

COATZACOALCOS, VER. JUNIO DEL 2009

AGRADECIMIENTOS

A DIOS POR OTORGARME LA SABIDURIA Y EL ENTENDIMIENTO POR GUIARME EN ESTE CAMINO DE EXITO.

A MIS PADRE: POR CADA CONSEJO QUE ME HAN BRINDADO Y POR EL APOYO INCONDICIONAL EN CADA MINUTO DE MI VIDA

INDICE

PROBLEMA

¿Cómo se puede saber si el firewall esta funcionado correctamente, al no pasar información no autorizada?

HIPOTESIS

La certidumbre de que no pueden entrar hacker a la red, de no sacar información importante, de no tener virus en nuestro servidor, al igual puede brindarnos conocimientos en la seguridad de herramientas para proteger una red de ataques.

OBJETIVOS GENERALES

Establecer un firewall correctamente a la red con el servidor, para que los intrusos (hackers) no puedan tener acceso sobre la información que se tiene en dicha re.

OBJETIVOS ESPECIFICOS

- Dar un mejor servicio a la red
- Proteger a la redes, controlar que recursos externos pueden utilizar los usuarios.
- Este es una seguridad que nos brinda firewalls para los ataques que se dan en la red.
- El firewall permite al administrador de red dar acceso a los usuarios de la red a distintas tipos de servicios de internet.
- Esta selectividad es una parte esencial de cualquier programa de gestión de información e implica, no solo la protección de información privada, si no el conocimiento de quien acceda a dicha red.

JUSTIFICACION

El porqué realizar este tema es para saber su principal función de firewall. Y cuál será sus objetivos generales, y conocer más del tema ya que a veces no se sabe cómo proteger su red.

Su principal función es un dispositivo como firewall entre redes es una barrera defensiva entre las redes ya que permite o negar la transmisión de una red privada y el internet. Cuando algo a alguien puede tener acceso a tu computadora en cualquier momento, tu computadora es susceptible de ser atacada, puede restringir el acceso externo a tu computadora y a la información contenida en ella con un firewall. Además de la existencia de 2 formas de seguridad tanto en hardware como en software.

Y sus objetivos generales son:

- Proteger a las redes, controlar que recursos externos pueden utilizar los usuarios.
- Este es una seguridad qué nos brinda firewalls para los ataques que se dan en la red.
- El firewall permite al administrador de red dar acceso a los usuarios de la red a distintas tipos de servicios de internet.
- Esta selectividad es una parte esencial de cualquier programa de gestión, si no el conocimiento de quien accede a dicha red.

INTRODUCCION

Durante mucho tiempo la seguridad es una de las prioridades para cada individuo, actualmente se ha evolucionado y se ha creado en diferentes aéreas la seguridad es una de las importantes, sobre todo en el área de la seguridad informática, ya que actualmente la información se considera como uno de los trabajos más valioso en cualquier entidad u organización. Para tener una seguridad informática realmente efectiva, se requiere de un estudio especifico de las entidades dependiendo de las actividades que cada uno de los individuos realice dentro de su organización desean conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios se ha incrementado el número de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso de worl wide web (www) , acceso a los servicios de Internet Mail (e-mail), Telnet y File Transfer Protocolo (FTP). Adicionalmente la mayoría de los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso público en el Internet.

Es un hecho que las necesidades de cada entidad sobre seguridad informática difieren de los requerimientos de cualquier entidad ya sea una de la otra.

La propia naturaleza de cada uno de estos elementos sobre todo el que se refiere a “individuos” hace que cada modelo de seguridad informática sea particular, la cual los administradores de la red tienen que incrementar todo con respecto a la seguridad de sus sistemas para cada individuo en una organización, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los expertos de Internet. Para tener un mejor nivel de protección se requiere que la organización siga una política de seguridad, para prevenir el acceso no autorizada de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Aun todavía si una organización no está conectada al Internet, esta debería establecer una política de seguridad interna, muy estricta, para administrar el acceso de usuarios a porciones de red y proteger la información confidencial de cada organización.

El firewall es un dispositivo que funciona entre redes, es una barrera defensiva entre las redes ya que permite o negar la trasmisión de una red privada y el Internet. Cuando algo o alguien pueden tener acceso a tu computadora en cualquier momento, tu computadora es susceptible de ser atacado. Puede restringir el acceso externo a tu computadora y a la información de seguridad tanto en hardware como un software.

Aunque los firewall sean correctamente configuradas pueden ser eficaces en el bloqueo de algunos datos, no debe caerse en una falsa ser eficaces en el bloqueo de algunos datos, no debe caerse en una falsa sensación de seguridad. Aunque ofrezcan realmente una cierta cantidad de protección, los firewall no garantizan que su computadora no será atacada. En particular, un firewall ofrece poca o ninguna protección contra virus que trabaja haciendo que el usuario ejecute el programa infectado en su computadora, como muchos virus de correo lo hacen. Sin embargo usando un firewall junto

con otras medidas de protección (como software antivirus y practicas seguras de computo) reforzando su resistencia a ataques.

Mientras la seguridad global tenga una estrategia se requiere de la integración armoniosa de las personas, tanto el proceso, como la tecnología reduzcan el riego, no hay ninguna duda que los firewall pueden ser una muy valiosa herramienta de seguridad en cuanto se implementen apropiadamente. Hoy el uso de firewall se ha vuelto una práctica aceptada que se despliegue como si fuera la moda de forma virtual cuando se está diseñando y construyendo las redes. Reconociendo a estas necesidades, los sistemas de cisco, ha desarrollando y han seguido el contendido mejoramiento en su firmemente demostrando una mezcla excelente de funcionalidad, en la actualidad y de la gran flexibilidad de su producto en el mercado.

Los firewall se han vuelto los dispositivos en aumento sofisticado como la tecnología. En su nivel más básico, se piensa que un firewall de fuerza a una política de seguridad gobernada el trafico de la red que se atraviesa. A esto la funcionalidad básica de cisco, ha agregado muchos rasgos como la traducción de dirección de red virtual privada las redes (VPN), y arquitectura redundante para los sistemas.

Capitulo 1

MARCO TEÓRICO

Un firewall es un punto de comprobación entre una red privada y una o más redes públicas. Es una pasarela que decide selectivamente que pueda entrar o salir en una red privada, para ello, el firewall debe ser la única pasarela entre la red que protege y el exterior. Si el tráfico no pasa a través del firewall, la seguridad que este suministra no tiene ningún valor. Un principio básico es que todo el tráfico externo debe pasar a través del firewall. Un enrutador normal puede servir como cortafuegos si se configura como un punto de contención.

Tipos de firewall

Firewall de capa de red o de filtrado de paquetes

Firewall de capa de aplicación [1]

Firewall personal

Limitaciones de un Firewall

- Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de su operación.
- El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El cortafuego no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas.
- El firewall no puede proteger contra los ataques de ingeniería social.
- El firewall no puede protegerse contra los ataques posibles a la red interna por virus informáticos.
- La solución real esta en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

- El firewall no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a internet.

La autorización es el proceso de aprobación de derechos de acceso a un usuario, grupo de usuarios o sistemas específicos.

El control de acceso es el que limita el flujo de la información de los recursos de un sistema exclusivamente a las personas o sistemas de la red.

La integridad de los datos garantiza que los datos no han sido alterados ni destruidos por personas cuya misión consiste en modificarlos rotundamente.

La confiabilidad de los datos garantiza que únicamente las entidades con autorización para ver los datos, los ven con formatos usables.

El firewall proporciona filtro de paquetes con y sin estado, gestión basada en navegador, perfiles de seguridad predefinidos, filtro/bloqueo de puertos, administración remota y un asistente de configuración muy fácil de usar. A esto se añaden funciones antipirateo para evitar diferentes tipos de ataques como son las falsificaciones de direcciones IP, la interceptación de contraseñas, la manipulación de la caché de ARP y la suplantación de servidores, todas ellas medidas de seguridad importantes para las redes corporativas. En un entorno empresarial, un firewall de PC con funciones anti pirateó puede reducir las brechas de seguridad originadas internamente e impedir que los PC generen tráfico no autorizado. El resultado es una mejora global de la seguridad con menos intervención del personal técnico.

CAPITULO 2

ANTECEDENTES

No hace mucho tiempo una red de cómputo era algo que no muchas empresas o escuelas tenían en su centro de cómputo. La gran mayoría estas computadoras se encontraban aisladas una de la otra aunque se encontrarán en el mismo cuarto o salón de cómputo. Únicamente grandes empresas, instituciones gubernamentales o universidades tenían este recurso. Eso cambiando con el paso del tiempo y hoy en día es común encontrar computadoras conectadas a una red y obtener información de ella o brindar servicios (tal es el caso de internet o una intranet en una oficina u hogar), y es común el uso de ellas, como por ejemplo enviar y recibir correo electrónico, entre muchos servicios más.

El gran desarrollo de estas redes no ha sido del todo positivo en varios aspectos. Uno de ellos es la disponibilidad de Direcciones I, que esta limitado a 4300 millones de direcciones IP válidas aproximadamente. Esta cantidad de direcciones puede ser a primera vista muchísimas direcciones, pero direcciones válidas libres en internet son actualmente muy pocas, por lo que cada vez es más difícil poder obtener una dirección válida en internet. Con la llegada de la versión 6 del protocolo IP se espera poder extender este rango de direcciones en un part de millones más. Pero como esta nueva versión aun no se encuentra disponible debemos trabajar con la actual y por ende debemos administrar mejor el uso de este tipo de direcciones. Una forma de administrar mejor esto, es escondiendo computadoras con direcciones no válidas dentro de una red, detrás de una dirección IP válida. A ésta técnica se le conoce como enmascaramiento de direcciones.

Existe otro problema que no es técnico sino social. Cada día existen más computadoras y personas que accesan a internet. La necesidad de proteger los sistemas conectados a una red de usuarios no deseados es cada vez más común y se vuelve más importante día a día.

Instalar un firewall es en buena medida una solución para protegerse de ataques a una red interna o de usuarios no deseados. Actualmente, el kernel de Linux (por ejemplo Linux PPP 6.2, RedHat 6.2) soporta filtrado de paquetes, que pueden ser utilizados para implementar un sencillo firewall.

Un firewall constituye una especie de “barrera” delante de nuestro equipo que examina todos y cada uno de los paquetes de información que tratan de atravesarlo. En función de unos criterios establecidos (reglas) previamente el firewall decide que paquetes deben pasar y cuales deben ser bloqueados.

Muchos tipos de firewall son capaces de filtrar el tráfico de datos que intenta salir de nuestra red al exterior, evitando así que los diferentes tipos de código malicioso como troyanos, virus y gusanos, etc., sean efectivos. El firewall actúa de intermediario entre nuestro equipo (o nuestra red local) e internet, filtrando el tráfico que pasa por el.

Todas las comunicaciones de internet se realizan mediante el intercambio de paquetes de información, que son la unidad mínima de datos transmitida por la red. Para que cada paquete pueda llegar a su destino, independientemente de donde se encuentren las máquinas que se comunican, debe llevar anexa la información referente a la dirección IP de cada máquina en comunicación, así como el puerto a través del que se comunican. La dirección IP de un dispositivo lo identifica de manera única dentro de una red. El puerto de comunicaciones es una abstracción lógica que podríamos comparar con la frecuencia en una emisión radiofónica: del mismo modo que no podemos escuchar una emisora si no sintonizamos su frecuencia, no podremos conectarnos a un servicio de otro equipo si no usamos el mismo puerto.

Un firewall, como ya se ha descrito, intercepta todos y cada uno de los paquetes (todas las comunicaciones de internet se realizan mediante el intercambio de paquetes de información, que son la unidad mínima de datos transmitida por la red) destinados a/o procedentes de nuestro equipo, y lo hace antes de que ningún otro servicio los pueda recibir.

Para que cada paquete pueda llegar a su destino, independientemente de donde se encuentren las máquinas que se comuniquen, debe llevar anexa la información referente a la dirección IP de cada máquina en comunicación así como el puerto a través del que se comunican. La dirección IP de un dispositivo lo identifica de manera única dentro de una red. Por lo tanto, de lo anterior podemos concluir que in firewall puede controlar todas las comunicaciones de un sistema a través de internet.

Se dice que un puerto de comunicaciones esta abierto si cuando llega un paquete de petición de establecimiento de conexión, el sistema devuelve una respuesta. En caso contrario el puerto se considera cerrado y nadie podrá conectarse a el.

La verdadera potencia de un firewall reside en el que al analizar cada paquete que fluye a través del mismo, puede decidir si lo deja pasar en uno u otro sentido, y puede decidir si las peticiones de conexión a determinados puertos deben responderse o no.

Por ejemplo, si en nuestro equipo tenemos alojada una página Web personal podemos configurar un firewall para que sólo permita las comunicaciones a través del puerto de Web (puerto 80 y utiliza el protocolo HTTP), ya que es el único puerto que necesitamos.

En el intercambio de datos a través de internet los paquetes contienen un bit de reconocimiento, a través de cual se puede determinar si un paquete procede de una conexión ya establecida o es un intento de penetración externa. De esta forma es relativamente sencillo que un firewall pueda dejar pasar aquellas comunicaciones que el sistema interno haya establecido, impidiendo todas aquellas cuyo origen sea el exterior.

Los firewalls también se caracterizan por su capacidad para mantener un registro detallado de todo el tráfico e intentos de una conexión que se han producido. Estudiando los registros es posible

determinar los orígenes de los posibles ataques, descubrir patrones de comunicación que identifican ciertos programas maliciosos. Sólo los usuarios con privilegios administrativos podrán acceder a estos registros, pero es una característica que se le puede exigir perfectamente a éstas aplicaciones.

CAPITULO 3

INTRODUCCIÓN A LA SEGURIDAD Y FIREWALL

Análogamente, un firewall, en un sentido más informático, es un sistema capaz de separar el habitáculo de nuestra red, o sea, el área interna de la misma, del posible incendio de crackers que se produciría en ese gran motor que es internet.

3.1 LA IMPORTANCIA DE LA SEGURIDAD

La seguridad en red es una cuestión bastante y compleja y debido a la importancia de la seguridad tiene una amplia gama, ya que en la actualidad hay muchas soluciones para proteger, tanto nuestra PC, como a la red y los mecanismos de transporte de datos de la infraestructura de una red corporativa, ya que muchas de las tecnologías se pueden utilizar de un modo diferente de solucionar, como relacionarlos con la identidad del usuario o el dispositivo así como con la integridad de los datos y la confidencialidad de los datos.

Se dice que cada persona o dispositivo es una entidad misma que tiene capacidades distintas en la red y al que se le permite acceder los recursos de la red en base a quien es. Aunque en sentido amplio la identidad sólo le importa la autenticación y el control de acceso de las entidades.

La autenticación es el proceso de validación de la identidad reivindicada por un usuario final un dispositivo (como los clientes, los servidores, los switches, los routers, los firewalls, etc.) en otras palabras se dice que la Autenticación es el que asegura que los usuarios son, de hecho, quien ellos dicen que son.

Las contraseñas, son la manera antigua de autentificar a los usuarios, pero otros métodos de criptografías esta encargado de encriptar la información Y encriptar documentación no es otra cosa, que cambiar su forma y sentido de la información para que otra persona sea capaz de entenderla (cifrado, descifrado, clave pública o privada) y sistemas biométricas es una de las tecnologías de seguridad para solucionar de identificación y el control del acceso (estos utilizan características físicas del usuario como emisión de calor, huella digital, mano, cara, retina, voz)

La autorización es el proceso de aprobación de derechos de acceso a un usuario, grupo de usuarios o sistemas especifico.

El control de acceso es el que limita el flujo de la información de los recursos de un sistema a exclusivamente las personas o sistemas de la red.

La integridad de los datos garantiza que los datos no han sido alterados ni destruidos por personas cuya emisión con sostén en modificarlos rotundamente.

La confidencialidad de los datos garantiza que únicamente las entidades con autorización para ver los datos, los ven con su formato usable.

Se dice que las contraseñas se suelen utilizar para la autenticidad del usuario, es muy fácil descifrarlas si son fáciles de adivinar, si no se cambian con frecuencia, pero dentro de una entidad deben tener la seguridad de cambiarla por lo menos cada inicio de mes. Dentro de nuestra PC podemos tener seguridad mediante los antivirus, tenemos el poder habilitar dentro de nuestra PC nuestra seguridad con los servicios que utiliza el internet entre los cuales se encuentran------, DNS este es el más importante ya que en este se guarda la información de las veces que entre a las PC.

3.2 LA INSEGURIDAD Y LA INTERNET

De una federación de redes se organiza un grupo lo que hoy es el internet que estaba conformado de una comunidad relativamente pequeña de usuarios por los años ochenta, que se dedicaba únicamente a la investigación y con respecto a las comunidades. Porque era bastante difícil de hacer el acceso a estos sistemas al de las comunidades del usuario eran bastantes estrechamente el tejido, la seguridad no era de mucha preocupación en este ambiente. El objetivo principal de conectar varias redes juntas era sola para poder compartir la información. Las tecnologías como el sistema operativo UNIX y la transmisión controla el protocolo/El protocolo de internet conectado una red de computadoras protocolos que se diseñaron para esto, el ambiente reflejo esta falta de preocupación de seguridad. La seguridad simplemente fue vista como innecesaria.

Por los tempranos 1990, sin embargo, el interés comercial en el internet había crecido. Estos intereses comerciales tenían las perspectivas muy diferentes en la seguridad, la información comercial tenía el valor, y acceso a el necesitó ser limitado a las personas específicamente autorizados, **UNIX, TCP/ IP** y las conexiones a la internet se volvieron avenidas de ataques y no tenían mucho la capacidad para llevar a cabo y dar fuerza a confidencialidad integridad y a la disponibilidad. Como la internet creció en la importancia comercial, con el número de compañías se querían conectar a el, incluso el edificio los modelos de negocio enteros alrededor de el, la necesidad para la seguridad aumentada se puso bastante aguda. Las organizaciones conectadas enfrentaron las amenazas ahora que ellos nunca habían tenido que considerar antes.

Las amenazas crecen cuando el ambiente de la informática corporativa era un cerrado y limitado-acceso el sistema las amenazas vinieron principalmente de dentro de las organizaciones. Estas amenazas interiores venían de los empleados enfadados con acceso privilegiados que podría causar

mucho daño. Los ataques del exterior no eran mucho un problema desde que había típicamente solo unos. Potencial los asaltadores se dice que el 99% de los hackers o asaltadores de información se encuentran dentro de la misma organización ya que el uso limitado de la información hacen que en la actualidad el administrador de la red tenga un dio fin de firewall para proteger la información debido a que con la información pueden hacer un mal uso o dañar el desempeño de terceras personas. Además con el crecimiento de la internet, las amenazas externas crecieron ahora millones de organizadores en la internet como blancos del ataque potenciales que inciten el ahora los números grandes de grupo de saltadores. Estos han crecido en el tamaño y habilidad durante los años cuando sus miembros comparten información adelante como interrumpir en los sistemas para la diversión y ganancia. La geografía ya no sirve como un obstáculo. Usted puede atacarse a los continentes desde millas de distancia así como fácilmente como de su propio pueblo. Las amenazas pueden ser clasificadas como estructuras o falta de estructuras. Las amenazas de falta de estructura son de las personas con la habilidad baja y perseverante. Estas normalmente viene de niños de la estructura llamado que tiene poco o ninguna habilidad de la programación y el mismo conocimiento del sistema pequeño.

Los asaltadores estructurados son los famosos compumaniaticos que se dedican simplemente a dar lata, y cumplir sus metas u objetivos de triunfo. En la que se incluye robo de código de la fuente, el robo de tarjeta de crédito, o fraude, robo del sueldo.

La ingeniería social, también conocida como las personas que se dedican a tajar, los medios para la información de seguridad obtenida de las personas que las engañan. El clásico el ejemplo está llamando a un usuario y está pretendiendo ser un administrador del sistema.

El cómputo maniaco le pregunta al usuario su contraseña para realizar alguna hostilidad, alguna tarea de mantenimiento importante. Para evitar a ser tajado vía la ingeniería social, eduque su comunidad del usuario que ellos siempre deben confirmar la identidad de cualquier persona que los llama y que las contraseñas nunca deben se dé a cualquier encima del correo electrónico, mensajería instante o teléfono.

3.3 CONCEPTOS DE FIREWALL

Un firewall es un punto de comprobación entre una red privada y una o más redes públicas. Es una pasarela que decide selectivamente que puede entrar o salir de una red privada. Por ello, el firewall debe ser la única pasarela entre la red que protege y el exterior. Si el tráfico no pasa a través del firewall, la seguridad que este suministra no tiene valor. Un enrutador normal puede servir como cortafuego si se configura como un punto de contención. La figura 3.1 muestra como actúa un firewall como un túnel a través del que debe todo el tráfico.

La palabra firewall viene del mundo de la arquitectura. Esta definición aplicada a la informática ilustra bastante el propósito de estos sistemas. Un firewall es un sistema ejercer políticas de control de acceso entre dos redes, tales como su red LAN privada e internet, una red pública. El firewall define

los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un firewall puede considerarse más que una puerta cerrada con llave al frente de su red.

En su servicio de seguridad particular, los firewall son importantes porque les proporciona un único "punto de restricción", donde se puede aplicar políticas de seguridad y auditoria. Un firewall proporciona al administrador de la red, entre otros datos, información acerca del tipo y cantidad de tráfico que ha fluido a través del mismo y cuantas veces sea intentado violar la seguridad.

Mucha de la confuncion acerca de los firewall del gran numero de ellos que hay disponible en el mercado y la gran variedad de funcionalidad y complejidades que ofrecen. El abanico se extiende desde los dispositivos orientados a usuarios domésticos hasta sistemas complejos de nivel corporativos.

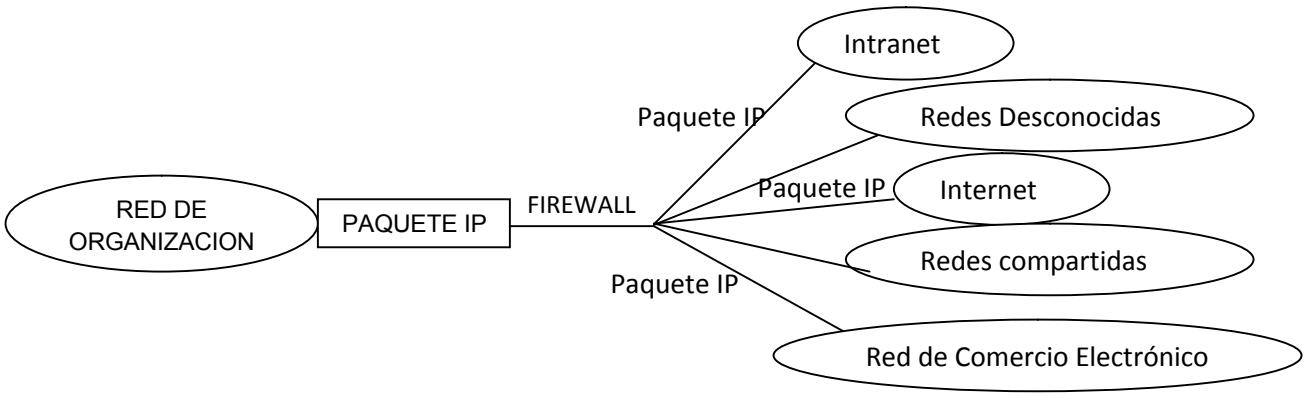


Figura 3.1 Un firewall se define en parte por su posición como cuello de botella del tráfico

3.4 FUNDAMENTOS DE LOS FIREWALL

Creación de las reglas de los firewall o políticas. El firewall, de hecho es una clase de enrutador. El tráfico entra a través de una interfaz de red, sale por otra y los mensajes se manejan o en la capa de una interfaz de red, sale por otra y los mensajeros se manejan o en la capa de red (nivel 3) del modelo OSI de 7 capas.

Los firewall funcionan interceptado e inspeccionada cada paquete que entra por cualquier de sus interfaces de red. La inspección varía dependiendo de la sofisticación del firewall y de lo exigente que sea la política de seguridad. Pero el objetivo es siempre identificar una coincidencia entre el

contenido de cada paquete y las reglas de seguridad con las que se han él firewall, para hacerlas cumplir. Los pasos fundamentales para interceptar e inspeccionar paquetes.

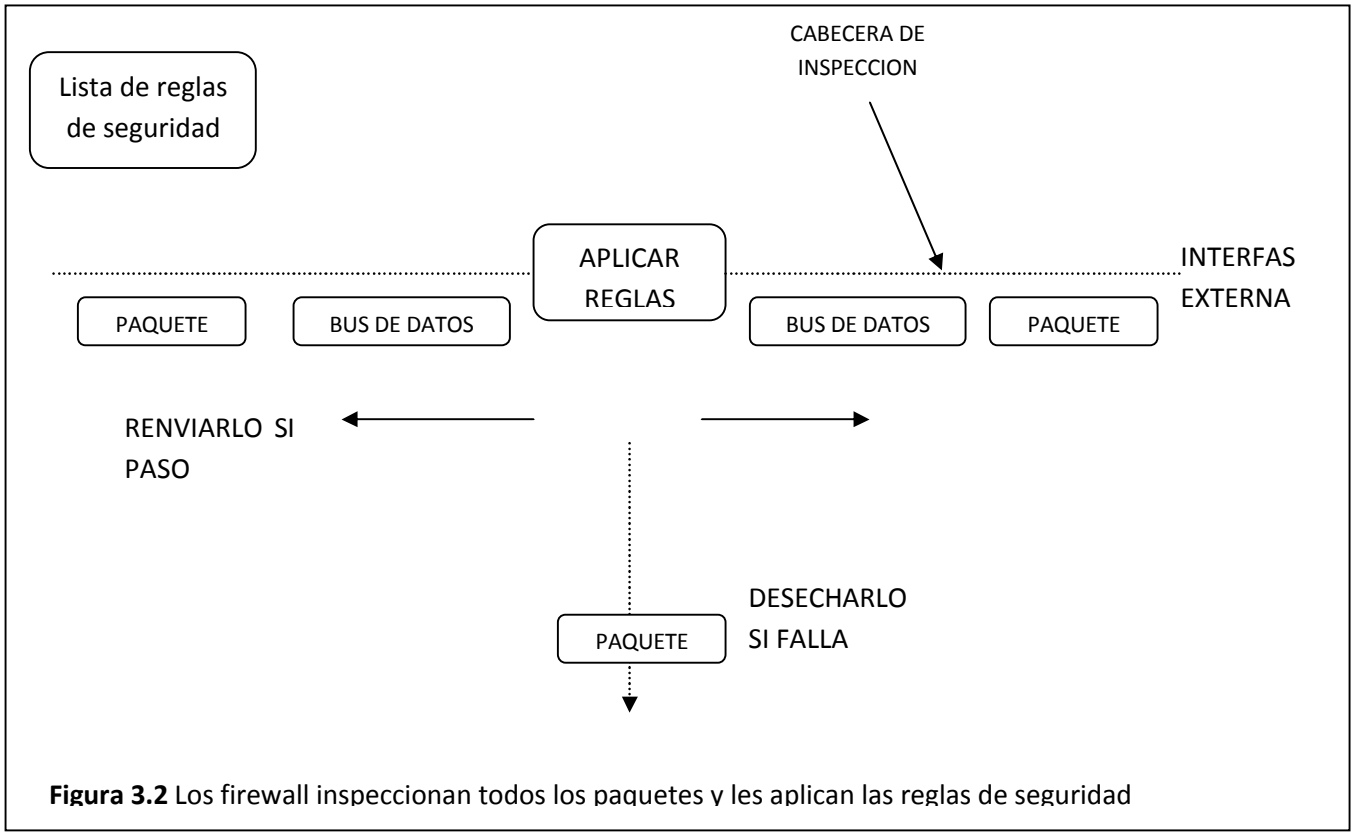


Figura 3.2 Los firewall inspeccionan todos los paquetes y les aplican las reglas de seguridad

La forma que tiene los firewall de interceptar el tráfico no es precisamente atractiva. Lo hacen canalizando todo el tráfico que entra en sus interfaces de red a través de una sola trayectoria (llamando bus de datos en la terminología de computación) obligando a que todo el trafico pase a través del bus de datos internos y de la memoria de los firewall, la unidad central de proceso (CPU) tiene oportunidad de comprobar que todos los paquetes cumplen las reglas de seguridad con los que se ha programado para hacer cumplir.

La inspección real se hace leyendo la cabecera del paquete para encontrar condiciones que coinciden con las reglas configuradas en las tablas de seguridad. Las tablas de seguridad suelen incluir docenas de reglas, cada una diseñada para aceptar o rechazar explícitamente clases especificadas de tráfico, aplicando una prueba de paso/fallo al paquete. Si el paquete lo pasa, se reenvía a su destino. Si falla, el paquete se desecha en la interfaz de red y deja de existir.

3.5 OBJETIVOS BÁSICO DE FIREWALL

En pocas palabras, un firewall lleva acabo tres funciones para proteger su red:

- Bloque los datos que pueden contener el ataque de un hacker.
- Oculta la información acerca de la red, haciendo que todo parezca como si el tráfico de salida se originara del firewall y de la red. Esto también se conoce como NAT (Network Address Translation).
- Filtra el tráfico de salida, con el fin de restringir el uso de internet y el acceso a localidades remotas.

La forma habitual de garantizar de la infraestructura es a través de los firewall. Un firewall, en su sentido as amplio, controla el flujo de tráfico. Y se crean reglas para permitir o denegar los distintos tipos de tráfico y equilibrar las decisiones sobre enrutamiento tomadas. El permiso o la denegación del tráfico pueden incluir servicios de red específicos. Por lo regular, los firewall son implementaciones en los puntos de entrada y salida de la infraestructura de la red.

3.5.1 NIVELES DE FILTRACIÓN

Un firewall puede filtrar tanto el tráfico que sale como el que entra. Debido a que el tráfico que entra constituye una amenaza mucho mayor para la red. Este es inspeccionado mucho más estrictamente que el tráfico que sale. Al momento de evaluar productos de hardware y software, los filtros de un firewall se define a partir de cierto criterios, tales como:

- Dirección IP. Se puede bloquear el acceso desde un IP específica, evitando ataques o consultas a equipos, servidores y clientes.
- Nombre de dominio. Consiste en tablas con nombres de computadoras vinculadas al DNS a donde no se permite el acceso de los usuarios locales.
- Palabra clave. Programas detective en los firewall revisan el contenido de la información en búsqueda de palabra vinculadas con información o sitios no permitidos.
- Puertos, cada aplicación o servicio que usa la red IP genera una conexión hacia un puerto. El 80 es el común para los servidores WWW y el 21 para la transferencia de archivos. Un firewall registra estos servicios, que computadoras pueden acceder a ellos y cuáles no.
- Protocolo, es factible restringir el uso de algunos protocolos como http (el que sirve las paginas WWWW) o telnet (para sesiones remotas). Así se evita que usuarios mal

intencionados del exterior de la red. Intenten acceder a un equipo local mediante un protocolo específico.

Para un administrador de firewall es mucho más sencillo aplicar el filtrado por puertos o protocolos que los anteriores, dado que los métodos 1 al 3 requieren de más vigilancia y administración del firewall, aunque método excluya a los demás de ser empleados.

Imágenes que los niveles de filtración son un proceso de eliminación. El firewall inicialmente determina si la transmisión entrante ha sido solicitada por un usuario de la red y, de no ser así la rechaza. Luego, cualquier dato que haya sido permitido se inspecciona cuidadosamente. El firewall verifica la dirección de la computadora del remitente, con el fin de certificar que proviene de un sitio confiable. Finalmente se encarga de verificar el contenido del a transmisión.

3.6 TIPOS DE ATAQUE DEL EXTERIOR AL INTERIOR

Antes de definir exactamente qué tipo de firewall necesita, debe entender la naturaleza de los tipos de amenazas de seguridad que existen sujetos buenos y malos. Los sujetos malos abarcan desde individuos incompetentes que provocan daños sin intenciones hasta hacker habilidosos y maliciosos que planean ataques que pueden potencialmente impactar en forma negativa a su negocio.

- Hurto de información. Robo de información confidencial, tales como registros de clientes y empleados, o hurto de propiedad intelectual de su empresa.

- Sabotaje de información, cambios a l información en un intento de dañar la reputación de una persona o empresa. Como por ejemplo, elaborando o publicando contenidos males intencionados en su sitio web.

- Negación de servicio. Bloqueo de los servidores o red de su empresa, de forma que los usuarios legítimos no pueden acceder a la información o, para impedir la operación norma de su empresa.

Intentos para lograr Acceso

Un hackers puede intentar obtener acceso a su red por diversión o ambición. Un intento de lograr acceso, por lo general, comienza con la recolección de información acerca, por lo general comienza con la recolección de información acerca de la red. Luego, esta información se utiliza para realizar un ataque con u propósito especifico, ya sea para apoderarse o destruir datos.

Un hacker puede usar un scanner de puertos, un software que permite ver la estructura de la red. Esto les permite averiguar como esta estructurado la red y que software se esta ejecutando de la red, puede aprovecharse de todas las debilidades conocidas del software y utilizar las herramientas de “hacking” para ocasionar estragos en su ambiente de TI.

Es posible ingresar a los archivos de los administradores y dejar en blanco los discos, aunque una buena calve de acceso por lo general puede dificultar esta tarea.

Afortunadamente, un buen firewall es inmune de un escaneo de puertos y a medida que se desarrollen nuevos scanner de puerto para evadir esta inmunidad. Los fabricantes de firewall producen actualizaciones para preservarla.

Ataques de negación de Servicio (Dos, Deniel of service)

Los ataques dos son puramente maliciosos. No producen ningún beneficio para el "hacker" mas que el placer, de que las redes o parte de ellas queden inaccesibles para sus usuarios. Un ataque dos sobrecarga el sistema de manera que lo deja inhabilitado, negando así la posibilidad de utilizar los servicios de la red. Los hackers envían grandes paquetes de datos o programas que requieren que el sistema responsa continuamente a comandos falsos. Para llevar a cabo un ataque Dos, un hacker tiene que conocer la dirección IP del sistema que va a atacar, pero un buen firewall no revela su propia dirección IP o las direcciones de la red. El hackers puede pensar que se ha constatado con el firewall y, desde ese punto, no es posible bloquear la red. Así mismo, cuando un hackers lanza un ataque, algunos firewall pueden identificar los datos como tal , rechazar los datos, alertar al administrador del sistema y realizar un seguimiento de los datos, para capturar al individuo que los envió.

3.7 CAPA EN LA QUE TRABAJAN LOS FIREWALL

Para diferenciar los tipos de firewall tendremos que tener primero en mente el modelo ODI de redes:

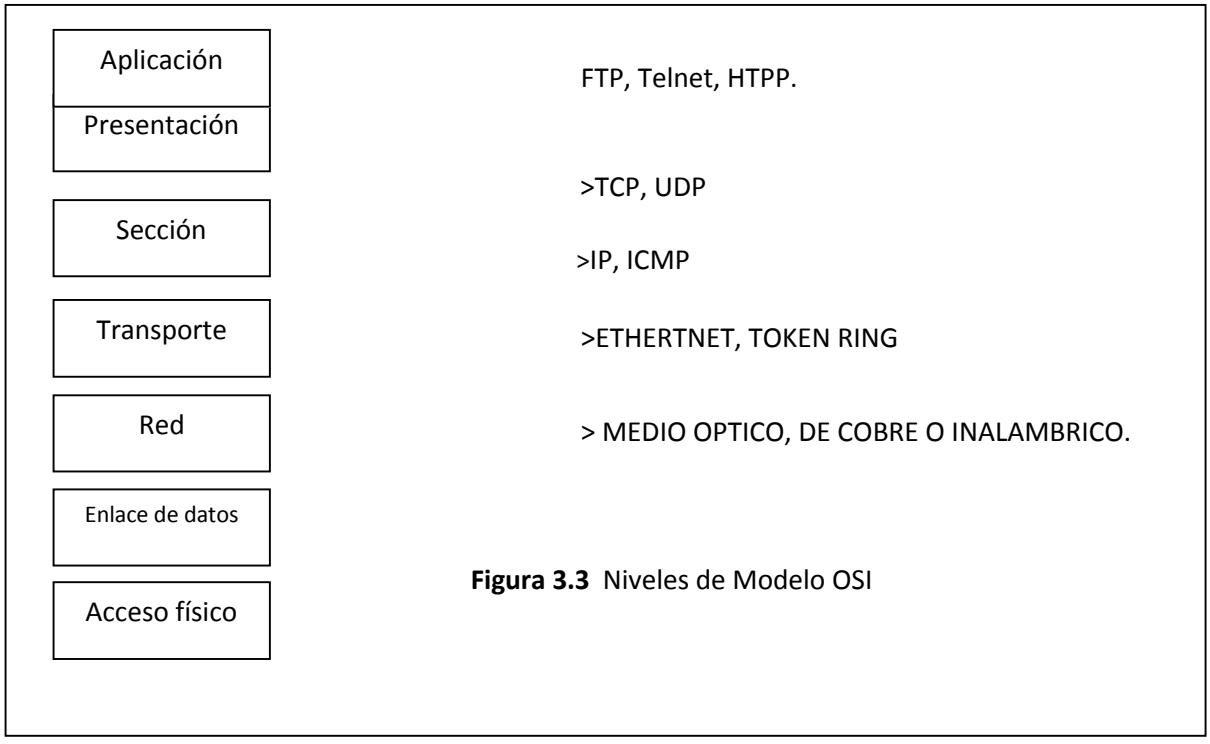


Figura 3.3 Niveles de Modelo OSI

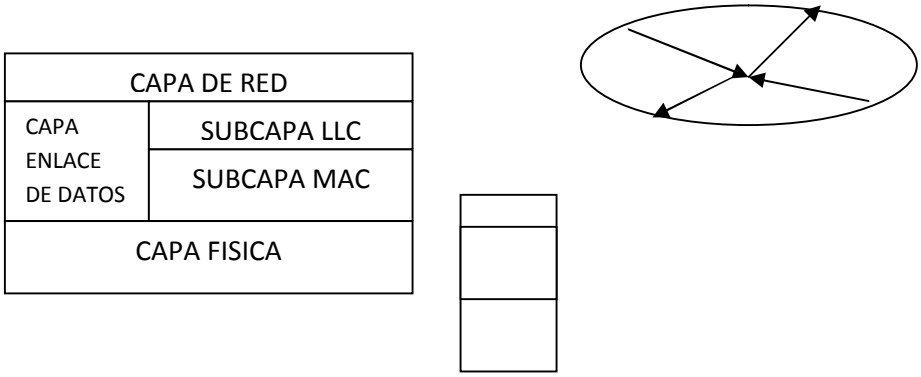


Figura 3.4 Equipos de Comunicación de nivel de Red.

CAPITULO 4

ESTABLECIMIENTO DE UNA POLITICA DE SEGURIDAD DE FIREWALL

Al discutir las políticas de seguridad es necesario hablar acerca de los riesgos. Debido a que los riesgos son la antítesis de la seguridad, naturalmente luchamos para eliminarlos. Sin embargo, a pesar de lo valioso que sea este objetivo, con cada experiencia aprendemos que la eliminación completa nunca es posible.

4.1 EVALUA LOS RIESGOS DE SEGURIDAD EN SU CORPORACION

Es útil pensar en la administración de riesgos para utilizar alguna clase de formula por supuesto, no se trata de una ecuación matemática que se puede utilizar con el fin de hacer determinaciones cuantitativas del nivel de riesgo y para evaluar el nivel cualitativo del peligro que representa una situación determinada.

La confiabilidad y los pasos necesarios para permitir y lidiar con las fallas en la confiabilidad son aspectos de la administración de riesgo que se debe tomar en consideración. En la seguridad de los sistemas de información, la palabra “amenaza” describe un componente de riesgo más limitado. Para ese propósito. Las amenazas se realizan por organizaciones o individuos que intentan causar daño y que tienen la capacidad de cumplir con sus intenciones.

Para desarrollar una política de seguridad cuidadosa es necesario considerar las posibles consecuencias de ataque desde una amplia variedad de amenazas, en donde cada una pueda actuar en un punto vulnerable especifico diferentes a otros intentos que no hayan sido reconocidos. Comúnmente, las amenazas a la información y a los sistemas de información y a los sistemas de información van a la par con una línea de ataque especifico o con un conjunto de puntos vulnerables, debido a que una amenaza que no tiene la capacidad de aprovechar los puntos

vulnerables no genera riesgos; es útil manejar la pareja amenaza-punto vulnerables en el proceso de administración de riesgos.

Al asumir que la amenaza es capaz, decidida y componente, al evaluar que contamos con objetivos altamente potenciales y al estimar en forma conservadora las incertidumbres, reducimos la administración de riesgos a "¿Cuáles son nuestros puntos vulnerables y cual es el costo de las medidas preventivas para eliminarlos?"

A fin de cuentas, el proceso de administración de riesgos consiste en tomar decisiones. El impacto de un ataque con éxito y el nivel aceptable de riesgo en una situación determinada fundamentalmente son decisiones de política. La amenaza, cual quiera que esta sea, puede ser abatida, controlada o atenuada. Pero se encuentra más allá del control directo del proceso de seguridad. Por lo tanto, el proceso debe enfocarse en los puntos vulnerables y en las medidas preventivas. Los puntos vulnerables son aspectos del diseño y debe eliminarse durante las etapas de diseño, desarrollo, fabricación e implementación de las instalaciones, el equipo, los sistemas y las redes. A pesar de que la distinción no siempre es muy clara, las medidas preventivas son menos características de los sistemas que de los entornos y de la forma en que se les utiliza. Por lo general, hacer que algún valor sea menos vulnerable eleve su costo no solo en las fases de diseño y de desarrollo, ya que también requiere validaciones y pruebas más extensas con el fin de asegurar la funcionalidad y la utilidad de las características de seguridad, y requiere de medidas preventivas durante las fases de operación y mantenimiento.

° Físicos: causados por el acceso no autorizado de las personas a un centro de computo, lo cual permite examinar cosas a las que no debería tener acceso. U buen ejemplo de esto sería un navegador instalado en un lugar público (como la recepción de una empresa)que le proporciona al usuario la oportunidad de navegar en la web, pero también de cambiar, pero también de cambiar la configuración y proporcionar información del sitio como las direcciones IP, los registros DNS, etc.

° Software: son causados por aplicaciones "con errores privilegiadores" como los daemons que ejecutan funciones que no deberían. Como regla general, ¡nunca confié en scripts ni en applets! Cuando las los utilice, asegúrese de comprender cual es su función (¡y qué es lo que no deben de hacer!)

° Aspectos de compatibilidad: causados por la mala planeación de la integración del sistema. El hardware o el software pueden trabajar muy bien en forma independiente, pero una vez que se reúnen con otros dispositivos, como un sistema, pueden representar problemas. Estos problemas son difíciles de detectar una vez que las partes se integran en el sistema. Es mejor que se asegure de probar todos los componentes antes de integrarlos en el sistema.

° falta de política de seguridad : no importa que tan seguro sea su mecanismo de autenticación de contraseña si sus usuarios utilizan los nombres de sus hijos como contraseña .Es necesario contar

con una política de seguridad que establezca todos los requisitos para la seguridad de un sitio y que cubra y evite todos los agujeros posibles en la seguridad.

Los requisitos para contar con un firewall seguro también incluyen una serie de “buenos hábitos” que usted, como administrador, debe seguir .una buena regla consiste en hacer que las políticas se mantengan simples. Así serán más fáciles de mantener y de modificar, en caso de que sea necesario.

La mayoría de las aplicaciones para host y firewall cuentan con la capacidad para generar registros en bitácora de tráfico.

° La dirección IP

° nombre del servidor/host

° El tiempo de transferencia de información

° El nombre del usuario (si es conocido por la autenticación del usuario o. con UNIX, si es obtenida por el protocolo identd)

° El URL solicitado

° La variables de datos enviadas atreves de los formularios que los usuarios llenan durante una sesión.

° El estado de la solicitud.

° El tamaño de los datos transmitidos

Por lo tanto, un problema fundamental al desarrollar una política de seguridad consiste en vincular las características de diseño que reducen los puntos vulnerables y las medidas preventivas contra las amenazas , con el impacto que se genera al crear un balance efectivo que permite obtener un nivel aceptable de riesgo. El proceso se desarrolla de la manera siguiente.

1. Evaluar el impacto de las perdidas o de los daños en el objetivo potencial.
2. No todos los daños son económicos
3. Especifique el nivel de riesgo por el daño o por la destrucción que sea aceptable
4. Identifique y caracterice la amenaza.
5. Analice los puntos vulnerables
6. Especifique las medidas preventivas
7. Espere y permita las incertidumbres
8. Recuerde que, en la práctica, las estimaciones necesarias para aplicar los procesos de administración de riesgo solo se obtiene en términos amplios.

4.2 SEGURIDAD DE LOS DATOS.

Los bastion hosts (y en ese caso también los servidores) ¡son torpes! Son obedientes y harán lo que usted les pida que hagan, pero por desgracia, son torpes.

Debido a que no piensan por su propia cuenta, ni saben diferenciar entre el administrador del firewall y un hacker. (Bueno, ¡nosotros probablemente sabríamos que hacerlo¡) cualquier cosa que se coloque dentro del directorio raíz del documento del bastion host estará expuesta y protegida si usted no encuentra una forma de protegerla.

Los bastion host que cuenta con una gran cantidad de características y de ser vicios opcionales son especialmente propensos a los riesgos de seguridad de los datos.

Sin embargo, cuando seleccione su sistema operativo, tenga en cuenta a la seguridad de los datos ¡y también a la seguridad del sitio! Asegúrese de que el sistema operativo cuente con opciones solidas de seguridad de acceso.

Al enfrentarse a la web, el soporte proxy le ayudara a prevenir los ataques o a los visitantes indeseables, lo cual mejorara la seguridad de los datos. También le ayudara a hacerlo frente a los agujeros que generalmente se abre debido a características peligrosas que están en muchos paquetes de software para servidores Web.

Otros aspectos importantes que se debe considerar es el sistema operativo subyacente del servidor web es un aspecto vital al determinar que tan seguro es el servidor frente a los ataques de los hackers.

La apertura inherente de un sistema UNIX implicara trabajo extra cuando trate de bloquear el acceso a los hackers. A su vez, un sistema basado en Mac es mucho más seguro ya que no es tan abierto como un sistema UNIX.

Además del sistema operativo, deberá tener cuidado con las características que cada sistema ofrece. Existen características potencialmente peligrosas que se deben desactivar, en especial si no se necesitan. A continuación se presentan una lista de características que se deberán vigilar con mucha atención:

- Listados de directorio automático: Entre mas sepa un atacante acerca del sistema mayores posibilidades tendrá de modificarlo. Por supuesto, los listados de directorios automáticos pueden ser muy convenientes, pero los hackers pueden obtener acceso a la información más delicada a través de ellos. Entre esta información se incluye:

  -Archivo de sistema

  -Bitácoras de control de acceso

-Directorios con archivos temporales

Asegúrese de desactivar los listados de directorio automático, aunque eso no evitara que los hackers puedan capturar los archivos cuyos nombres hayan adivinado, pero por los menos hará que el proceso sea más difícil.

- Seguimiento de vínculos simbólico: Existen servidores que permitan extender el árbol de documentos con vínculos simbólicos. A pesar de que son convenientes, pueden ser peligrosas si el vínculo se crea con un área delicada.

- Inclusión del lado servidor: Uno de los principales agujeros en la seguridad que se presenta en los servidores web es la forma "exec" de la inclusión del lado servidor. Se deberá desactivar por completo o solo deberá estar disponible para los usuarios confiables.

Otra forma de proteger los datos es a través del uso de SSL, el cual utiliza un encriptado de llave pública para intercambiar la llave de una sesión entre el cliente y el servidor. Debido a que cada transacción utiliza una llave de sesión distinta, incluso si un hacker desencripta la transacción, la llave secreta del servidor seguirá protegida.

Si cuenta con un programa servidor FTP no comprometerá la seguridad general de los datos al compartir directorios entre este programa y el programa servidor de la web. Sin embargo, ningún usuario remoto deberá subir archivos que después puedan ser leídos o ejecutados por el servidor web. De otra forma, un hackers podría colocar un script CGI en el sitio FTP y después utilizar su navegador para solicitar el nuevo archivo cargado desde el servidor web, lo cual haría que el script se ejecutara y se omitiría la seguridad. Por lo tanto, limite todas las colocaciones de archivos del servidor FTP a un directorio que no pueda ser leído por los usuarios.

4.3 LA AMENAZA DE LOS VIRUS

Consideramos el problema de los virus de computadoras. Se estima que existen cerca de 15,000 virus en circulación y que un 85 por cierto de todas las redes corporativas han estado infectadas en algún momento. Los virus son tan persistentes que se han logrado detectarlos en programas de software empaquetadas directamente por el fabricante. Lo pregunta no es "¿Cuándo recibiré un virus?¿Porque no adquiere un programa de software antivirus?.

Por supuesto, los virus solo son programas y se pueden detectar al analizar las secuencias de instrucciones características que conforma la parte del programa que realiza las copias y que las envió para extender la infección, o la parte que se encargaba del trabajo sucio, la carga que despliega un mensaje molesto o que destruye los datos. Además, en ese lugar radica el problema. El software antivirus debe ser enseñado a reconocer la cadena de instrucciones del virus para poder determinarlo.

Por supuesto es posible actualizar el software antivirus cuando se descubra nuevos virus o nuevas versiones de virus antiguos; pero siempre se trata de un juego de persecución, y ni siquiera los usuarios que tienen la precaución de actualizar sus programas con frecuencia estarán completamente protegidos.

Los programadores que crean virus se mantienen actualizados con el software antivirus mas novedoso y constantemente mejoran su tecnología para los ataques. En la actualidad se han encontrado virus que encriptan su código para evitar la detención. Otros virus utilizan la tecnología de compresión para facilitar su trasmisión y para hacer que el reconocimiento sea mas complicado. Esos cambios dan como resultado virus que se conocen como ”polimorfos” debido a que constantemente cambian las características especiales que hubieran facilitado su detección. También hemos comenzado a encontrar virus que reconocen si el software antivirus se esta ejecutando buscan los sectores del dispositivo de almacenamiento que ya han sido limpiado y se copian dentro de dichos sectores, con lo cual se evita el rastreo de software antivirus. Por lo tanto, a pesar de que el software antivirus es valioso y esencial (es parte de un buen programa de seguridad para la información), no es suficiente por si mismo.

La política practicas y procedimientos de seguridad como los que se discuten en este capitulo, pueden reducir los riesgos hasta in nivel que se pueda manejar. Algo más peligroso son los riesgos que representan las amenazas directas, como las que genera los adversarios con capacidad y disposiciones para atacar la confidencialidad la integridad y la disponibilidad de los sistemas de información.

4.4 DENTRO DE LA AMENAZA

En los lugares en que los sistemas de seguridad de información de alta calidad regulan las transacciones de datos entre los limites que separan a los sistemas y a las redes de una organización del ciberespacio sin reglas, y que protegen la confidencialidad, la integridad y la disponibilidad de los sistemas de información de una empresa puede ser mas sencillo y económico utilizar a un empleado para que realice un ataque directo. El atacante también puede buscar empleo en esa empresa y contar con el acceso con el cuenta como empleado.

Todas nuestras defensas se dirigen a los ataques externos. Pocos sistemas cuentan con gran equipamiento de firewall interno que regulan las transacciones de información dentro de una empresa. Muchos sistemas proporcionan la capacidad de supervisar y auditar las transacciones de información, incluso las que solo se realizan dentro del sistema.

Sin embargo, buscar a un usuario interno que esta abusando de sus privilegios entre el enorme numero de las transacciones que se realizan en forma rutinaria es una tarea abrumadora que se vuelve imposible cuando no se cuenta con técnicas basadas en computadoras para reducir las auditorias y establecer análisis.

Es por eso que la mayoría de nuestros problemas son internos. Las técnicas se describen en capítulos posteriores y ayudan a abatir los riesgos resultantes, incluyendo el buen uso de la ciencia de la computación y la criptografía para proteger los valores y los sistemas de información, supervisar y auditar con el fin detectar las intrusiones por parte de usuario externos o internos, y contar con una capacidad efectiva para reaccionar frente a los incidentes relacionados con la seguridad, corregir problemas y trabajar con operaciones seguras. Pero una seguridad efectiva y eficiente dependerá de que existan políticas de seguridad apropiadas.

4.5 COMENTARIOS ACERCA DE LOS AGUJEROS EN LA SEGURIDAD

Los agujeros en la seguridad son una de las principales amenazas que deberán cubrir las políticas de seguridad, en especial debido a que muchos de ellos no se corrigen con el uso de un firewall. A continuación se presentan los diversos tipos de agujeros en la seguridad que amenazan la seguridad de una red.

- Agujeros físicos en la seguridad: Son causados por otorgarle acceso físico a una maquina a las personas que no cuentan con autorización, ya que esto les permitirá ejecutar acciones que no debería realizar.

- Agujeros de software en la seguridad: Son causados por un error en el código de aplicación o en el software “privilegiado”, el cual puede ser manipulado para que haga cosas no debería hacer. El ejemplo más famoso de esto es el agujero “sedmail debug” que podría permitir que un in cracker generara un proceso del intérprete de comando con los permisos del súper usuario. Esta acción se podría utilizar para borrar el sistema de archivo, crear una nueva cuenta, copiar el archivo de contraseñas y muchas otras cosas.

Los agujeros en la seguridad son difíciles de predecir, de detectar y de eliminar. A continuación se presentan una lista de sugerencias sobre como evitarlos y estar preparada para ellos.

- Si usted trabaja con u servidor UNIX, intente estructurar el sistema para que la menor cantidad posible de software se ejecute con los privilegios de los usuarios, lo cual se conoce como algo muy robusto.

- Suscríbase a una lista de correo en donde obtener detalles sobre los problemas o soluciones con la mayor rapidez posible y asegúrese de instalar todos los parches tan pronto como estén disponibles.

- No instale ni actualice ningún sistema o servicio a menos que este seguro de que los necesita. De otra forma podría estar abriéndole la puerta a los hackers. Muchos paquetes incluyen daemins o herramientas que puedan revelar información para los usuarios

externos. Además muchos paquetes TCP/IP instalan y ejecutan problemas en forma automática como rwhod, fingerd y tftpd, todos los cuales presentan problemas para la seguridad.

- No confié en los scripts de instalación. Muchos de ellos tienden a instalar o a ejecutar todo lo que se encuentran en el paquete sin preguntarle al usuario. Por lo tanto, revise la lista de programas que se incluyen en el paquete antes de comenzar con la instalación.

- Busque los agujeros en la seguridad que se generan por el usuario incompatible de hardware y de software. En muchas ocasiones, debido a la falta de experiencia, un administrador puede instalar software en donde existan problemas de compatibilidad y eso puede dar como resultado fallas en la seguridad. El agujero se genera por tratar de conectar dos elementos útiles que son incompatibles. Los problemas de esta índole son muy difíciles de detectar una vez que el sistema se instala y comienza a funcionar, de tal forma que es mejor construir el sistema en cuenta este tipo de problemas.

Como lo comento Gene Spafford "existe un cuanto tipo de problemas de seguridad que se relacionan con la percepción y con al compresión. El software perfecti, el hardware protegido y los componentes compatibles no funcionaran a menos que se seleccione una política de seguridad apropiada y que se activen las partes del sistema para aplicarse" y añade "el hecho de contar con el mejor mecanismo de contraseñas del mundo no sirve para nada si los usuarios piensan que escribir en forma inversa su nombre de usuario en una buena contraseña. La seguridad se relacionan con una política (o conjuntos de políticas) y la operación de un sistema de ejecutan de acuerdo a dicha política".

Para encontrar agujeros en la seguridad e identificar las debilidades en el diseño es necesario comprender la estructura y los niveles de control del sistema. Para poder hacerlo siempre es necesario tratar de:

- Determinar cuales son los elementos que se protegerán a los objetos de seguridad, como los archivos de los usuarios.

- Identificar los objetos de control o los elementos que protegerán a los objetos de seguridad.

- Detectar los agujeros potenciales en un sistema. Estos agujeros son frecuencia se encuentran en el código

-Se transportan para un nuevo entorno de programación o sistema operativo.

-Recibe alimentación de argumentos o datos de manera inesperada.

- Interactúan con otro software local.

-Realice pruebas al código para observar su comportamiento ante fuentes de datos inesperados: cobertura, flujo y mutación.

4.6 CONFIGURACION EN LA POLITICA DE SEGURIDAD

Un firewall para Internet no es un dispositivo autónomo: es parte de la política de seguridad general de una organización, la cual define todos los aspectos de su perímetro de defensa. Para tener éxito, las organizaciones deben conocer que es lo que están protegiendo. La política de seguridad deberá estar basada en un análisis de seguridad bien dirigido, así como en una evaluación de los riesgos y en un análisis de las necesidades del negocio. Si una organización no cuenta con una política de seguridad detallada, el firewall mejor construido podrá ser burlado para exponer a toda una red privada frente a un ataque.

Una plantilla con una política de seguridad típica. Utilícela como una base para su propia política de seguridad, añada o elimine cualquier aspecto que considere necesario y asegúrese de contar con un contacto estrecho con los administradores, ya que ellos deberán apoyar totalmente esta política.

4.6.1 PLANTILLA PARA UNA POLITICA DE SEGURIDAD

1-.Propósito: Esta regulación establece los requisitos de seguridad mínimos que la universidad utilizara Internet. Esta regulación no ha sido diseñada para restringir el uso de Internet, si no para garantizar que existe la protección adecuada para asegurar los datos de frente a los intrusos, la manipulación de archivos, los ataques y la interrupción del servicio.

Este tipo de actividades puede ser difícil de descubrir y de corregir, puede representar una gran vergüenza para la organización, y puede ser muy costoso en términos de perdida de la productividad y de arriesgar la integridad de los datos.

Todos los usuarios de Internet necesitan estar consientes del alto potencial de amenazas que existen en Internet y de los pasos de deberían tomar para asegurar sus sitios un mayor nivel de seguridad y de protección.

2-.POLITICA: La responsabilidad de proteger los recursos de la universidad en Internet corresponde a los departamentos de sistemas de información y de tecnología o de administración de los sistemas

de información. Esta política se aplica a los contratistas y universidades que se conectan a una computadora de la universidad. El departamento de la universidad que accede a Internet deberá desarrollar e implementar una política de seguridad para Internet que cumpla con los requisitos mínimos de esta regulación de la siguiente forma:

- Todo el personal de la universidad que utiliza a Internet deberá seguir las guías que se presentan en documentación adicional.
- El personal de la universidad que planee utilizar una gateway independiente para Internet será responsable de instalar, implementar y mantener la protección señalada, incluyendo el diseño y la implementación de un programa amplio par la administración de riesgo.

3-. La seguridad basada en servidor será el método principal para proteger los sistemas de la universidad. Sin embargo, muchos paquetes de software de seguridad basados en servidor no son confiables para protegernos en Internet debido a que son vulnerables frente a los ataques de negación del servicio.

4-. Debido a las debilidades inherentes en cierto servicios de telecomunicaciones para Internet y a algunos aspectos extraños en los paquetes de seguridad, muchos sitios descubrirán que el método mas practico para asegurar el acceso a sus sistemas desde Internet consiste en utilizar una gateway segura o un sistema de firewall. Las oficinas sucursales y los departamentos de la universidad deberán realizar evaluaciones de los riesgos con el fin de determinar los lugares mas adecuados para las Gateway, firewalls, tarjeta inteligentes o señales de autentificación.

- Utilizar firewalls o filtros de paquetes en los enrutadores locales cuando el sistema utilice TCP/IP.
- Configurar los firewalls con acceso de salida hacia Internet, pero limitar estrictamente el acceso de entrada a los datos y sistemas de la universidad por parte de los usuarios de Internet.
- La falla en el firewall podría ser desastrosa para la seguridad de una subred. Por esta razón las oficinas sucursales deberán, siempre que sea práctico, adherirse a la siguiente lista de estipulaciones cuando configuren y utilicen firewalls.
- Limitar las cuentas de firewall a solo aquellos que sean absolutamente necesarios, como las de administrador. Si es practico, desactive los inicios de sesión de red.
- Utilizar tarjetas inteligentes o señales de autenticación para proporcionar un mayor grado de seguridad que el se podría obtener con una contraseña sencilla. Las tarjetas de respuesta a

las solicitudes y de contraseñas únicas se integran con facilidad en los sistemas más populares.

- Remover los compiladores, los editores y otras herramientas de desarrollo de programas del sistema de firewall que pudieran permitir que un cracker instalara software de caballo de Troya o de puerta trasera.

- No ejecutar vulnerables en el firewall como TFTP,NIS, NFS O UUCP.

- Considerar la desactivación del comando finger. El comando finger se puede utilizar para crear fugas de información muy valiosas.

- Considerar dejar de utilizar los comandos de gateway para correo electrónico, los cuales pueden ser utilizados por los crackers para buscar las direcciones de los usuarios.

- No permitir auto-agujeros en los sistemas de firewall al otorgar a sistemas o usuarios conocidos acceso de entrada especial. Le firewall no deberá considerar como confiable ningún intento por obtener acceso a las computadoras detrás de el.

- Desactivar cualquier característica del firewall que no sea necesario incluyendo el acceso a otros redes, los programas de interacción con el usuario las aplicaciones.

- Desactivar las sesiones con interpretes de comandos complementarios funcional en el firewall y leer los registros de bitácoras por lo menos cada semana.

- Ninguna computadora o subred de la universidad que cuente con conexiones hacia Internet podrá almacenar información privada o delicada sin utilizar firewall o algún medio para proteger los datos.

- Las afinas de la universidad deberán desarrollar y documentar una estrategia de seguridad para Internet basada en el tipo de servicio para Internet que se ha seleccionado. Esta estrategia se deberá incluir en el plan de seguridad para Internet.

- Todo el software disponible en Internet deberá ser revisado en busca de caballos de Troya o de virus de computadoras una vez que haya sido descargado en una computadora de la universidad.

- Es necesario contar con una evaluación obligatoria de los puntos vulnerables y los riesgos de las Gateway existente en intervalos anuales. La evaluación inicial se deberá completar en un plazo de nueve meses después de la expedición de esta política. Todas las oficinas sucursales deberá llevar a cabo revisiones semanales o mensuales de los registros de

auditoria del software de Gateway y de firewalls con el fin de buscar agujeros en la seguridad.

- Las computadoras host se deberán revisar periódicamente para asegurar que cumplan con los lineamientos de seguridad de la universidad.

5-.Responsabilidades:

- Desarrollar, coordinar, implementar, interpretar y mantener las políticas, procedimientos y lineamientos de seguridad en Internet para la protección de los recursos de sistemas de información de la universidad.

- Revisar la política de seguridad de Internet en la universidad.

- Ayudar en el desarrollo y la implementación de la política de seguridad en Internet de las oficinas sucursales de la universidad.

- Determinar las medidas de seguridad mas adecuada para los sistemas que se utilizan como Gateway hacia Internet.

- Asegurar que todas las oficinas sucursales de la universidad realicen evaluaciones periódicas de los riesgos de seguridad en los sistemas de información, evaluaciones, de seguridad, y revisiones de control internas de las Gateway y las instalaciones operativas para Internet de la universidad.

En las oficinas de la universidad que cuenten o que planeen instalar un firewall o cualquier tipo de firewall o cualquier tipo de Gateway Internet deberán:

- Desarrollar e implementar un extenso de administración de riesgo que aseguren que los riesgos para la seguridad se identificaran, se tomaran en cuenta y se mitigaran a través del desarrollo de controles de seguridad de bajo costo. El sistema de administración de riesgo incluirá una política de acceso al servicio que definirá aquellos servicios a los que se permitirá acceso o que quedaran fuera de una red restringida, la forma en que esos servicios se utilizaran y las excepciones a esta política.

- Otra parte del sistema de administración de riesgos consistirá en una política de diseño para el firewall. Esta política se relaciona directamente con los firewalls y define las reglas utilizadas para implementar la política de acceso del servicio.

- Cada oficina sucursal y cada oficina de personal deberá desarrollar un plan de seguridad para Internet que estipule todos los controles de seguridad que se encuentren instalados o que se planee instalar.

- Esos controles deberán relacionarse con los riesgos identificados por medio del análisis de riesgo. Los planes de seguridad para Internet deberán ser presentados cada año con los planes de seguridad de la universidad para su revisión y su aprobación. Los lineamientos que determinan la presentación de estos planes de seguridad deberán ajustarse al plan de seguridad para Internet.

El MIS de la universidad deberá ser responsable del desarrollo, la evaluación y el mantenimiento de los planes de contingencias para Internet. El riesgo relacionado con el uso de Internet hace que sea esencial contar con planes y procedimientos para:

- Reducir el daño y las interrupciones causadas por eventos no deseados.

- Garantizar el desempeño continuo de las funciones y los servicios esenciales para los sistemas.

- Desarrollar, instalar, mantener y revisar regularmente los registros de auditorias en busca de actividades poco usuales en el sistema.

- Crear, implementar y mantener las características de protección preescritas identificadas como una solución por parte de la evaluación de riesgos.

CAPITULO 5

MANTENIMIENTO DEL FIREWALL

El nivel de seguridad que ha implementado en la universidad directamente relacionada con la cantidad de dinero que ha invertido en el y con los riesgos que esté dispuesto a tomar. El manteniendo de un firewall comienza con su administración y, desde el punto de vista administrativo, no debe considerar que la instalación de un firewall es la solución para todos sus problemas de seguridad. Siempre debe recordar que, como se ha mencionado a lo largo de este libro, los firewall proporcionan una amplia variedad de herramienta de control, pero a final de cuentas solo con herramientas. Un firewall es parte de una estrategia de defensa diversificada que identifica que es lo que debe ser protegido y cuáles son las amenazas potenciales.

Parece obvio, pero existen más aspectos relacionados con la protección de una red que simplemente el hardware y el software. La seguridad proviene de la integración de la tecnología confiable con los administradores de redes activos y en estado de alerta, y con las decisiones administrativas relacionadas con el acceso de los usuarios a Internet y a otros recursos

computacionales. La prudencia exige el desarrollo de un plan muy completo para resolver los problemas de seguridad. Usted como el administrador de su red, junto con el personal de seguridad deberá definir por los menos los siguientes puntos.

- Que elementos de deben proteger.
- Los niveles de riego a los cuales están expuestos esos elementos.

Es por eso que sus políticas de seguridad deben incluir múltiples estrategias. Este concepto se emplea cada día más en la medida en que los administradores de redes consideran que las tecnologías y en especial los firewall, son una cuta total para la seguridad de sus instalaciones. Esta es una ruta arriesgada. Los firewalls no deben para realizar tarea cada vez más complejas y poco razonable, como el rastreo de paquetes en buscas de virus, el encriptado de los datos e incluso los idiomas extranjeros.

Sin embargo, de ningún modo debe descartarse el firewall. No solo porque el firewall este cumpliendo con su trabajo debe sin vigilancia. Al igual que un automóvil, para que funcione bien y de manera eficiente, necesitara cuidado y atención continuos. En ocasiones serán necesarios algunos arreglos y unas cuantas revisiones. Nunca descuide un firewall, Internet es un mundo salvaje.

Si actualmente su firewall está configurado para proteger a su corporación frente a amenazas conocidas, mañana tal vez aparezca alguna amenaza desconocida que podría generar problemas. El tiempo que deberá invertir para cuidar a su firewall variara. Dependerá del tiempo de firewall que haya instalado, de los valores que está protegiendo y del tipo de servicio de Internet, y del acceso que proporcione.

Algunas compañas confían en los enrutadores para el filtrar el tráfico de las conexiones no deseadas. Si este en su caso, entonces cuenta con un conjunto de reglas que no quieren de un mantenimiento muy complicado. Como se menciono antes, con este tipo de firewall se aceptan o se rechazan los intentos de conexiones. En este caso le tengo buenas y malas noticias. La buena noticia es que el tiempo que necesitara invertir para cuidar a su firewall es casi nulo. Además de permitir nuevas conexiones y de rechazar algunas otras, no hay nadad que puede hacer más que asegurarse de que el firewall este activado y de que las tarjetas NIC continúan funcionando, lo cual en caso de que se presentara alguna falla, se notaria de inmediato. La mala noticia es que tal vez tenga que evitar el acceso al tráfico deseado, como el de los clientes, potenciales y no podrá aprovechar la gran cantidad de servicios y recursos de Internet que se encuentran en el ciberespacio. Asegúrese de no contar con un mal representante en la administración de los sistemas de información.

Si su compañía es de las más importantes del mundo, será mejor que cuente con una política de seguridad integral y bien detallada; de otro forma, podría enfrentarse a muchos problemas. Por lo tanto debe sondear el tráfico de la red que llega al firewall desde Internet y mantener protegida a su red todos los días. Si las mediciones del tráfico de su red alcanzan los gigabytes. Es por eso que realizar este sondeo manualmente es casi imposible. Su firewall debe contemplar el sondeo del tráfico, las alertas de seguridad y las características de generación de informes.

Debido a que generalmente los firewall se encuentran en una posición ideal para obtener información estadística sobre el uso de la red, puesto que todo el tráfico debe pasar a través de ellos, es posible rastrear y analizar el uso del enlace a la red a intervalos regulares. Este análisis pude ayudarle enormemente a evaluar el uso de la red y su desempeño, así como cualquier amenaza en la seguridad y a conocer las medidas que debe tomar para resolver problemas.

Es posible analizar cuáles son los productos que están alcanzando el mejor desempeño, cuales son las subredes a las que se accede y, basándose en la información reunida, la programación de los servicios de actualización, la reparación de errores de programación o, si es necesario, descubrir los agujeros en la seguridad y eliminarlas.

Si cuenta un firewall de filtrado de paquetes, debe tener al menos un conocimiento básico sobre los protocolos de trasporte que cruzan a través del cableado con el fin de cuidar a su firewall. Con esto, como Alec Muffet lo describe correctamente en su informe, las reglas de filtrado que utilizara estarán destinadas a controlar el tráfico basándose en:

- Extremos de enlace de transporte, o una noción de lo que se encuentra dentro y fuera de la red. En el mundo de TCP/IP, esto se implementa al enmascarar parte de las direcciones de origen y de destino, y al comprobar si las porciones restantes de las direcciones hacen referencias a los hosts que se encuentran dentro de la red protegida.
- Protocolo de transporte, como RCP, UDP o IP único. Otros protocolos podrían contar con soporte directo o se podrían asumir que pasaran por un túnel a través del firewall.
- Opciones de protocolo que deben incluirse en cualquier firewall de buena calidad, el cual debe tener además la capacidad de “desechar” el trafico basándose en la opciones dependientes del protocolo que podrían comprometer la seguridad si se utilizan mal; por ejemplo, la opción de “enrutamiento de origen” de IP que se puede utilizar para falsificar el trafico. Además que al aspecto más importante en el filtrado de paquetes es la capacidad de hacer coincidir el trafico de la red con una tabla que contiene los hosts de origen y destino (o redes) permitidos, pero también es muy importante hacer notar que la revisión del firewall de debe realizar en ambos extremos de la conexión y se deben tomar en cuenta los números de servicio de los puertos en cada extremo de la conexión; de otra forma, el firewall podría ser atacado con facilidad.

5.1 MANTENGA SU FIREWALL BIEN AFINADO

Un firewall es algo parecido a llevar un automóvil al taller para que le den servicio de afinación. Al igual que con el automóvil, en el firewall la afinación es necesario debido a que le permitirá:

- Extender su vida útil
- Comprobar que se ejecuta en forma adecuada
- Asegurarse de que el firewall sigue proporcionando un ambiente seguro para la empresa.
- Optimizar su operación y sus servicios.
- Realizar cualquier actualización necesaria.
- Asegurar que los componentes del firewall siguen funcionando e interactuando entre si.

Al realizar una afinación periódica en le firewall, usted será capaz de evaluar de manera adecuada la carga de operación que el firewall esta soportando o su capacidad para enfrentar y anticipar problemas en el futuro. Al doblar su desempeño con respecto a un número cada vez mayor de carga de operación medida, usted podrá tener un buen panorama general sobre los signos vitales de su firewall.

A continuación se describe un procedimiento de afinación de un firewall:

1-. Supervise su firewall durante un mes y guarde todos los resultados. Entre mas archivos de bitácora claros y completos obtenga, mejores serán los resultados del examen físico de su firewall.

Al hacer esto, tendrá una buena idea cerca de la carga de operación que pasa por el firewall, sin importar que se trate de un firewall de nivel de paquetes o de aplicación. Si el firewall es de nivel de aplicación, el proceso deberá ser muy sencillo debido a que este tipo de firewalls proporcionan muchos informes acerca del sistema en forma predeterminada.

Si se trata de un firewall de nivel de paquetes, por ejemplo en enrutador, deberá desarrollar algún tipo de control de dimensiones de la bitácora.

2-. Clasifique las bitácoras de acuerdo a la hora del día. Note que durante algunas horas del día de la carga de operación alcanza puntos más altos que otros y que se muestran diferentes características de la carga. La clasificación de las bitácoras en intervalo de una hora ofrece una evidencia de esto.

3-. Grupos de archivos de bitácoras por servicios que contengan valores como los siguientes:

- Numero de mensajes de correo electrónico durante ese intervalo.
- Tamaño promedio de los mensajes de correo electrónico durante ese intervalo.
- Tiempo promedio entre la llegada del correo electrónico durante ese intervalo.
- Numero de visitas en la web durante ese intervalo.
- Tamaño promedio de los objetos recuperados desde la web durante ese intervalo.
- Tiempo promedio entre los accesos a la web durante ese intervalo.

- Numero de recuperación FTP durante ese intervalo.
- Tamaño promedio de los objetos FTP recuperados durante ese intervalo.
- Tiempo promedio entre los accesos a la web durante ese intervalo.
- Numero de recuperación FTP durante ese intervalo.
- Tamaño promedio de los objetos FTP recuperados durante ese intervalo.
- Tiempo promedio entre las recuperaciones FTP durante ese intervalo
- Numero de sesiones Telnet durante ese intervalo.
- Numero máximo de sesiones Telnet concurrentes durante ese intervalo.
- Cantidad del trafico NNTP de llegada durante ese intervalo.
- Cantidad del trafico NNTP de salida durante ese intervalo.
- Tiempo promedio entre las sesiones NNTP durante ese intervalo.

4-. Anote la carga de operaciones mas lata en cualquier de los intervalos para cada servicio cuando se presente.

Si usted colocara toda esa carga de operaciones en el firewall durante un solo intervalo, tendría una imagen muy clara de la peor situación de carga la podría enfrentarse.

5-. Las herramientas de implementación para generar estas cargas de operación a partir de registros existentes pueden ser bastantes directas y se pueden ejecutar en cualquier sitio en el que se desea realizar esta prueba. Es probable que los valores sean diferentes para cada sitio, aunque tal vez no variaran mucho. Diversos scripts expect o scripts PERL que utilizan información de archivos estáticos, podría simular la carga de operación que pasa a través del firewall sin tener que hacer realmente en trabajo.

6-. Después de realizar este procedimiento deberá tener un paradigma básico de “carga de trabajo por intervalo” para el firewall dentro del ambiente de red de la universidad, incluyendo escenarios de punto máximos y del “peor de los caos”. Con esta información a la mano usted será capaz de afinar a su firewall basándose en la suposición de “que pasaría si” aumentara la carga al observar que sucede con el rango de solicitud de servicio durante las horas de mayor y de menor uso.

Puede considerar que el resultado de “carga de trabajo por intervalo” es un confiable para su firewall debido a que realizaba la medición ¿no es así? El objetivo consiste en determinar hasta que punto puede llegar su firewall, partiendo del nivel mas bajo y máximo de carga para el firewall partiendo del nivel más bajo y máximo de carga para el firewall.

7.- Ahora puede diseñar una prueba de seguridad que invoque a los emuladores para que desarrollen el mismo modelo de carga. Los valores que debe controlar son los siguientes:

- Numero de carga de operaciones concurrentes para el servicio.
- Tamaño de los accesos para el servicio.
- Intervalo entre los accesos para el servicio.

8-. Ejecute la prueba de seguridad con la carga configurada para que iguale la carga de salida en un momento especifico que no sea el punto máximo pero que se aproxime.

9-. Compare los tiempos de ejecución con una carga de operación aproximada a la del punto máximo frente a la medición real de la carga en el punto máximo.

10-. Ejecute la prueba de seguridad para emular la carga máxima.

11-. Ahora compare los tiempos de ejecución para la carga máxima con los tiempos de ejecución de la medición real de la carga en el punto máximo.

12-. Ahora tiene una plantilla que le puede ayudar a afinar a su firewall y que esta basada en lo que ocurre al incrementar la carga del trafico por arriba de los valores reales medidos.

5.2 SUPERVISE EL FIREWALL

Las características de administración son esenciales para supervisar su firewall y para inspeccionar su funcionamiento.

Al supervisar su sistema, debe tomar en cuenta la protección de la confidencializacion de sus usuarios, la sensibilidad de sus dispositivos y, en general, la seguridad de la red. La mayoría de los firewall incluyen mecanismos de inspección, y algunos proporcionan autentificación y encriptado.

Una buena medida de precaución para evitar ataques y riesgos innecesarios en su firewall consiste en reducir al máximo al bastión host, dejándolo en el nivel más bajo de funcionalidad necesaria. Le

recomiendo que elimine todo el software que no sea necesario. ¿Para qué correr riesgos al ejecutar software comprometedor en el host más importante de su red? ¿Para qué tener ese software instalado precisamente en esa computadora?

5.2.1 OBSERVE LAS AMENAZAS QUE NO HAN SIDO SUPERVISADAS

Un firewall no es una solución completa. Necesitara otros elementos además del firewall para proteger realmente a su sitio. Por esto, el firewall tal vez no sea capaz de darle información cerca de todo lo que ocurren en su Gateway, quien sale, quien entra, especialmente, que es lo que entra por ejemplo, la mayoría de los firewall no ofrecen protección en contra de los mensajes de correo electrónico destinados a un usuario valido. Lo que pasaría con un mensaje de correo electrónico con archivos anexados. Un archivo anexado podría ser un caballo de Troya, es decir un applet pequeño y malicioso que podría desactivar a su firewall desde adentro o bombardear a su red protegida. Así que nunca considere que la instalación de un firewall es una solución completa para todas sus necesidades de seguridad.

Los firewalls pueden supervisar el tráfico, de manera muy efectiva, pero no ofrecen protección completa contra el contenido de la información. Una solución de seguridad completa requiere la implementación de medidas de seguridad en todo los niveles del uso de la red, desde el acceso a las aplicaciones (control de acceso y encriptado) a través del nivel de red (evitando el engaño y otras amenazas), hasta el nivel físico (restringiendo las conexiones no autorizadas hacia la red).

5.3 MANTENIMIENTO PREVENTIVO Y CORRECTIVO

Con el fin de mantener a su firewall es buen estado, debe realizar algunas tareas de mantenimiento y, al hacerlo, es muy importante que se mantenga en contacto con los proveedores, buscar informes sobre los parches de seguridad; consulte a proveedores acerca de ellos.

Las nuevas versiones de los parches para reforzar el sistema operativo de su firewall y, cuando aparezcan, aplíquenlas. Pero espere asegúrese de confirmar con su proveedor que el parche sea seguro y estable, ya que algunos causan más problemas que soluciones. Además, tenga cuidado con los parches falsos, ya que de vez en cuando encontrara que alguien ha creado un parche que en realidad es un caballo de Troya y que intenta como si se tratara de un parche real.

Por lo tanto, debe darle mantenimiento a su firewall con regularidad. Al hacerlo estará llevando a cabo dos tipos de mantenimiento: preventivo y correctivo. El mantenimiento preventivo es el que se realiza para permanecer seguro, el que esta rigiendo por la ley de Murphy (“cualquier cosa mala que pueda sucederle al sistema, sucederá”). El mantenimiento correctivo se realiza para resolver un

problema, tapar un agujero en la seguridad, repara alguna imperfección en el código del sistema y así por el estilo. Por lo general se lleva a cabo el proveedor lanza un nuevo parche, cuando se presenta alguna falla en el sistema debido a un desastre natural, o si la seguridad del firewall se ve comprometida como resultado de un ataque.

Las siguientes listas contienen los buenos hábitos, pasos y procedimiento que debe seguir para mantener a su firewall funcionando correctamente, e incluye medidas preventivas y correctivas.

- Respalde todos los componentes del firewall, no solo los bastion hosts que tiene instalado el software del firewall, sino también los enrutadores.

- Tenga cuidado cuando añada nuevas cuentas de administración en un firewall debido a que es muy importante mantener la seguridad del sistema del mismo. Las cuentas nuevas deben agregarse en forma correcta, además de que se deben eliminar las cuentas antiguas. Asegúrese de cambiar las contraseñas después de borrar una cuenta de usuario. Le recomiendo que limite el número de cuenta de usuario en el firewall, y que solo permita el acceso a los administradores.

- Revise las bitácoras de reporte del tráfico que pasa a través del firewall. La información siempre se expande para llenar todo el espacio disponible, incluso en las computadoras que tienen pocos usuarios. Por desgracia no existe ningún método para buscar basura dentro del disco en forma automática. Los programas de auditoría, como tripwire, le informara acerca de los nuevos archivos que aparezcan en áreas que supuestamente son estáticas. El principal problema con el espacio en disco lo representa las bitácoras del firewall. Estas pueden, y deben ser rotadas por las bitácoras antiguas que se han almacenado por lo menos durante un año.

- Supervise su sistema, si crea el habito de supervisar su sistema podrá determinar si: ¿El firewall ha estado bajo alguna clase de ataque si es así ¿Qué clase de ataques se han intentado en contra del firewall? ¿El firewall se resiste a esos ataques y funciones correctamente? ¿El firewall es capaz de proporcionar los servicios que los usuarios necesitan?

Supervise los intentos de utilizar los servicios que ha desactivado. Configure a sus sistemas para que grabe en bitácoras cualquier actividad relacionado con la seguridad. Si su firewall no incluye un software de auditoría uno, como tripwire y ejecútelo regularmente para descubrir los cambios inesperados en su sistema.

Registre sus eventos más importante e imprímalos cuando sea posible revise sus bitácoras con frecuencia, son muy importantes. Casi nunca encontraras algo sospechoso en ellas, pero algún día

podría encontrar evidencias de que algo malo sucede, y se sentirá feliz de haber enfrentado la difícil tarea de revisar las aburridas bitácoras.

- Ponga atención a las condiciones anormales de su firewall. Desarrolle una lista que incluye: todos los paquetes que fueron rechazados, información como la hora, el protocolo y el nombre de usuario de todas las conexiones exitosas hacia o a través del firewall. Todos los mensajes de error de sus enrutadores, firewall y cualquier programa de proxy.

5.4 EVITE LOS AGUJEROS EN LA SEGURIDAD DE SU FIREWALL

Muchos firewall de nivel de aplicación ya están construidos con la premisa de que evitar que ocurran problemas de seguridad en una red, es la mejor forma de resolverlos. Esta debe ser nuestra filosofía al implementar y mantener un firewall. Gran parte de los proveedores de firewall consideren que la prevención es un aspecto tan importante que muchos de ellos ya están integrados un sistema de rastreo de seguridad. En lugar de invertir en costosos auditorías externas de seguridad o realizar largas verificaciones internas, con interceptor usted confirmar que el firewall está haciendo su trabajo a través de internet scanner creado por internet el cual bombardea al firewall con intentos. Simulados.de irrupciones, internet scanner es una forma rápida y efectiva de verificar que interceptor está configurado correctamente y de que no se han omitido debilidades en la seguridad.

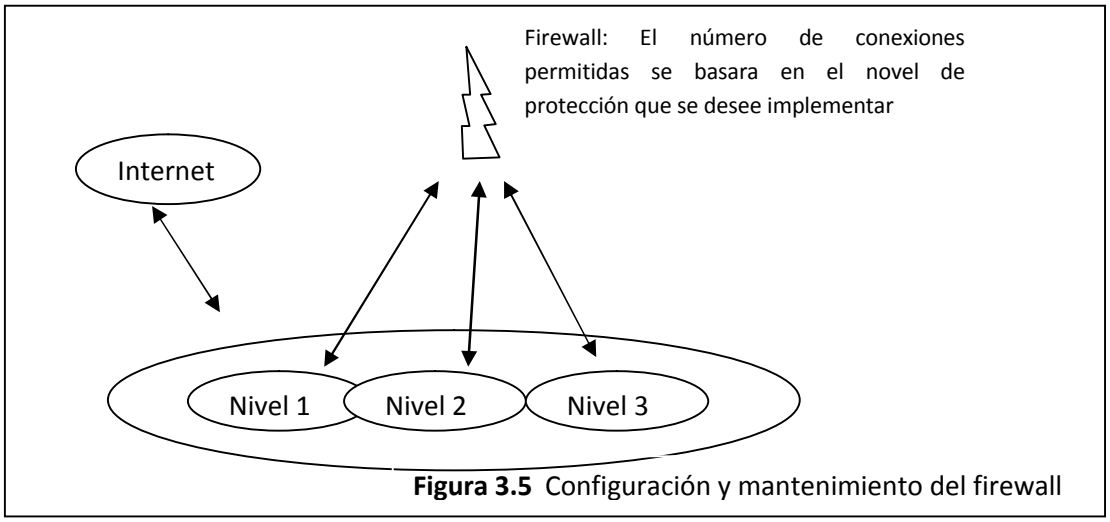


Figura 3.5 Configuración y mantenimiento del firewall

Como se describe anteriormente, otra medida de mantenimiento preventivo que se debe realizar periódicamente consiste en crear informes de revisión de seguridad. Estos informes pueden ayudarle aun más a identificar los problemas potenciales de seguridad en su sistema. Tipo de firewall y productos en el mercado, producen bitácoras detalladas de auditoría de toda la actividad del trafico de la red, así como otros informes de administración “fáciles de leer” sobre el acceso y la utilización de la red. Al revisar periódicamente estos informes se familiarizara con los patrones del uso de la red y podrá reconocer las aberraciones que incluso podrían producir problemas.

5.5 IDENTIFICAR LOS AGUJEROS EN LA SEGURIDAD

El primer paso importante que debe realizarse durante la instalación de un firewall, consiste en establecer una política de seguridad que define un uso aceptable. Como se configuran nuevas maquinas y aplicaciones, con frecuencia se pasan por lato los aspectos relacionados con la seguridad. Por lo tanto, el agujero entre la política central y la práctica descentralizada puede ser inmenso. Esto es a lo que me refiero con agujeros en la seguridad, los cuales también pueden ser generados por fallas en el sistema operativo o en las aplicaciones.

Si puede medir sus riesgos en la seguridad, entonces los puede controlar. El control efectivo de los riesgos en la seguridad solo puede ser implementado al evaluar el perfil de seguridad de la red. El proceso de auditar la seguridad, corregir los puntos vulnerables y supervisar continuamente las actividades, puede tapar casi por completo los agujeros en la seguridad que no estén relacionado con el sistema operativo o que no dependen de parches.

5.6 RECICLE SU FIREWALL

Al igual que cualquier otro componente de su red, los firewall también necesitan ser actualizados para que puedan seguir trabajando y responder a las nuevas amenazas. No es que debe ser pesimista, pero si considere que su solución de firewall es obsoleto el mismo día que la instala, será más capaz de enfrentarse a la constante necesidad de actualizar nuevos servicios que estén bajo la protección del firewall; si cuenta con un firewall de filtrado de paquetes. Incluso podría verse obligado a reciclarlo. Necesita tener acceso al correo y a los grupos de noticias en internet, a los proveedores y a otros usuarios para formar parte de la discusión acerca de los cambios en las practicas de seguridad de la redes. Además, necesita ayuda de los expertos para evitar caer en la tendencia de comprar cualquier sistema nuevo que aparezcan un servicio nuevo en su red tan pronto como sea anunciado por los proveedores. Es más seguro esperara y observar un poco mientras el mercado les “sacude los errores” y se desarrollen nuevas estrategias de seguridad. Pero, sin duda, su firewall no será eterno y eventualmente deberá reciclar o por lo menos actualizarlo. Para el caso de fallas en el sistema que no sean ocasionados por acciones intencionales de seres humanos, la meta principal de instalar un firewall se divide en tres partes:

1. Asegurar la persistencia
2. Proteger toda la información
3. Facilitar los servicios para lograr estas metas en su organización es necesario mantener archivos de respaldo de toda la información en un servidor de réplica, que se localice dentro del firewall.

CAPITULO 6

INTEGRACION DISEÑO E IMPLEMENTACION DEL FIREWALL

Diferentes tecnologías de firewall que se emplean en la actualidad, su fortaleza y sus debilidades, así como los sacrificios involucrados al diseñar un sistema de firewall e implementarlos de acuerdo a las necesidades especificas de las aplicaciones en todos los niveles de comunicación y solo extrae la información relevante, lo cual permite una operación bastante eficiente, el soporte para un numero de protocolo y aplicaciones y una extensibilidad sencilla para nuevas aplicaciones y servicios.

Las aplicaciones basadas en UDP al mantener una conexión virtual en la parte superior de las comunicaciones mantiene la información de estado para cada sesión a través de la gateway. Cada paquete de solicitud. Cada paquete de solicitud UDP que pase por el firewall quedara grabado, y los paquete UDP que viajen en la dirección opuesta serán comprobados con la lista de sesiones pendientes. Para comprobar que cada paquete UDP se encuentra dentro de un contexto autorizado. Un paquete que es una respuesta genuina a una solicitud se entrega y los demás se descartan. Si la respuesta no llega dentro del periodo especificado, la conexión termina. De esta forma, todos los ataques son bloqueados y las aplicaciones UDP se pueden utilizar de manera segura.

6.1 DESEMPEÑO DE FIREWALL

- Se ejecuta dentro del núcleo del sistema operativo, lo cual impone una sobrecarga insignificante al procesamiento. Además, no se requiere comunicación de contexto y se logra una operación con baja latencia.

- Emplea la técnica avanzadas para la administración de la memoria, como las talas de cache y de hash, las cuales se emplea para unificar instancias de objeto y ora hacer mas eficiencia el acceso a los datos.

- Sus mecanismos de inspección son genéricos y sencillos y se combinan con un optimizador de inspección de paquete, el cual asegura la utilización óptima de los diseños de la CPU y los sistemas operativos modernos.

De acuerdo con los resultados generados por pruebas independientes, la degradación del desempeño de una red al utilizar el firewall es demasiado pequeño como para ser detectado cuando opera a la velocidad completa de la LAN en la computadoras tipo SPARC de configuración mas baja firewall, soporta trabajo en red de lata velocidad, como ethernet a 100, con el mismo alto nivel de desempeño.

La metodología de prueba de diseño con cuidado para simular las condiciones reales, además de que utilizaron aplicaciones de automatización de pruebas para garantizar la precisión de los resultados.

Se evaluaron diversas configuraciones de firewall para determinar si el desempeño se veía afectado por el encriptado, la traducción de direcciones, los registros o el tamaño del conjunto de reglas. Además firewall fue obligado a trabajar con el número máximo de conexiones concurrentes que puede soportar. La opción fastpath fue activada en fiwerall para diversas configuraciones con el fin de maximizar el desempeño. Fastpath es una característica utilizada de firewall que optimiza el desempeño sin comprometer la seguridad.

Firewall se configura con dos interfaces de red: interna y externa. Cada interfaz utilizaba dos conexiones fase ethernet con el fin de maximizar el caudal de procesamientos y asegurar que firewall se esforzaba al máximo. Múltiples clientes en la red interna hicieron las solicitudes HTTP y FTP hacia múltiples servidores en el lado externo de firewall. Cada cliente genero cerca de 5 Mbps de tráfico y fueron añadidos incrementándose para aumentar el nivel del tráfico a través de firewall. Durante esta prueba un 75 por ciento de las conexiones eran http y el 25 por ciento restante eran conexiones FTP.

CAPITILO 7

LA DIVERSIDAD DE LOS FIREWALL

7.1 TIPOS DE FIREWALL

1-.Filtrado de Paquetes: Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

- Protocolos utilizados.
- Dirección IP de origen y de destino.
- Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

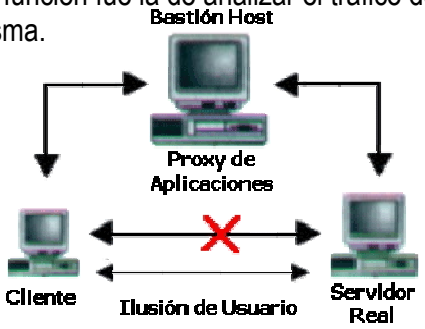
Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

- No protege las capas superiores a nivel OSI.
- Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
- Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
- No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

2-.Proxy-Gateway de Aplicaciones: Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

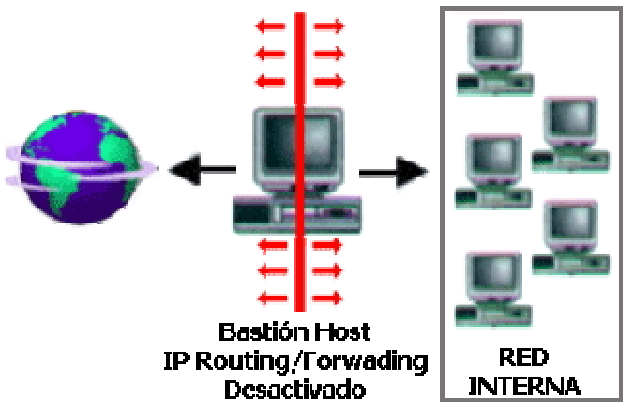
Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.



3-.Dual-Homed Host: Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".

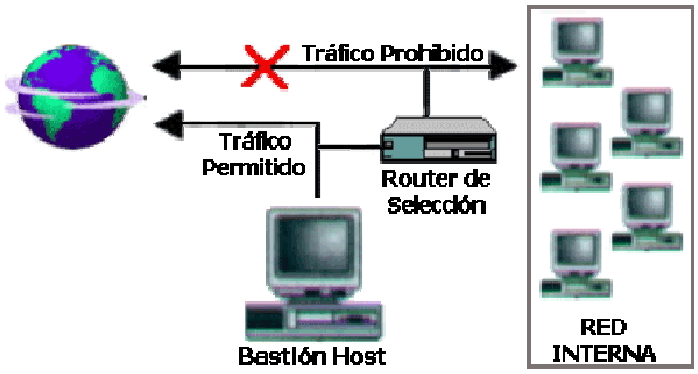
Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.



Estos Firewall son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

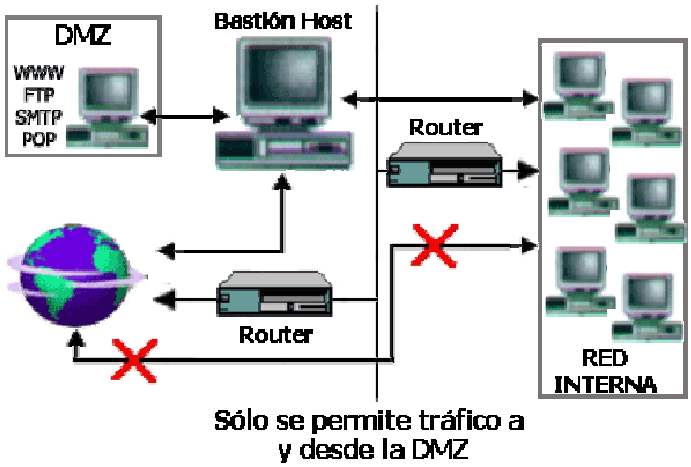
4-.Screened Host: En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.



5-.Screened Subnet: En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.

En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varias niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.



Como puede apreciarse la Zona Desmilitarizada aisla físicamente los servicios internos, separándolos de los servicios públicos. Además, n o existe una conexión directa entre la red interna y la externa.

Los sistemas Dual-Homed Host y Screnned pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

- Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
- Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
- Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red.

6-. Inspección de Paquetes

Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de

Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

7-. Firewalls Personales

Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

En la configuración de un firewall, la principal decisión consiste en corregir en elegir entre seguridad o facilidad de uso. Este tipo de dediciones es tomado en general por las direcciones de las compañías. Algunas firewall solo permiten tráfico de correos electrónicos a través de ellos, y por lo tanto protegen a la red contra cualquier ataque que no sea a través del servicio de correo. Otros son menos estrictos y solo bloquean aquellos servicios que se sabe que presentan problemas de seguridad.

Existen dos aproximaciones básicas:

- Todo lo que no expresamente permitida esta prohibido
- Todo lo que no es expresamente prohibido esta permitido

Es un primer caso de firewall se diseña para bloquear todo el trafico, y los distintos servicios deben ser activados de forma individual tras el análisis del riesgo que representan su activación y la necesidad de su uso. Esta política incide directamente sobre los usuarios de las comunicaciones, que pueden ver el firewall como un estorbo. En el segundo caso, el administrador del sistema debe que tipo de acciones pueden realizar los usuarios que pongan en entredicho la seguridad del sistema. Y preparar defensa contra ellas, esta estrategia penaliza al administrador frente a los usuarios pueden comprometer inadvertidamente la seguridad del sistema si no conocen y cumplen unas consideraciones de seguridad mínima. El problema se magnifica si existen usuarios que tengan cuenta en la propia maquina que hace firewall (situación muy poco recomendable).

En este tipo de estrategias hay un segundo peligro latente, y es que al administrador debe conocer todos los posibles agujeros de seguridad existentes en los protocolos y las aplicaciones que estén corriendo los usuarios. El problema se agrava debido al hecho de que los fabricantes no suelen darse prisa en notificar los riesgos de seguridad que presenta sus productos.

Firewall a nivel de Red

Por lo general se trata de un encaminador (router) o una computadora especial que examine las características de los paquetes IP para decidir cuales deben pasar y cuales no. Se podría configurar el encaminador para que se bloquease todos los mensajes que provengan del sitio de un determinado servidor de ese competidor. Los profesionales de redes a menudo denominan a este proceso lista negra. .

Normalmente se suelen configurar un encaminador para que tengan en cuenta la siguiente información para cada paquete antes de decidir si debe enviarlo:

- Dirección IP de origen y destino.
- Puerto origen y destino
- Protocolo de los datos (TCP, UDP o ICMP)
- Si el paquete es inicio de una petición de conexión.

Si se instala y se configura correctamente un firewall a nivel de red, este será muy rápido y casi totalmente transparente para los usuarios. Para servidores Linux un software que permite funciones de filtrado para implementar un firewall a nivel de red es el IP.

Firewall a Nivel de Aplicación

Suele ser un ordenador que ejecuta software de servidor Proxy. Por este motivo, los profesionales suelen referirse a el como servidor Proxy. La palabra Proxy significa actuar por poderoso o en nombre de otro. Los servidores Proxy hacen precisamente esto, se comunican con otros servidores del exterior de la red en nombre de los usuarios.

En otras palabras un servidor Proxy controla el tráfico entre dos redes establecidas la comunicación entre el usuario y el mismo y el ordenador destino. De este modo la red local quede oculta para el resto de Internet.

En algunos casos pueden controlar todas las comunicaciones de algunos usuarios con un servidor de la red. Un usuario que accede a Internet a través de un servidor Proxy parecerá para los otros ordenadores como si en realidad fuera el servidor Proxy (se muestra la dirección IP de este).

Como trabaja a nivel de aplicación, este tipo de firewall es mas seguro y potente, pero también menos transparente y rápido que un encaminador.

Existen servidores Proxy disponible ára diferentes servicios como http, Telnet FTP yGroper. A diferencia de los encaminadotes, es necesario configurar un servidor Proxy diferentes para cada servicio que se desee proporcionar.

Dos de los servidores Proxy mas populares para las redesbadasa un Unix y Linux son TIS Internet firewall Toolkit y Socks. Para servidores Windows tanto el Internet information Server de Microsoft, como el Comers Server de Netsacape incluye servidores Proxy.

Al implementar un servidor Proxy a nivel de aplicación los usuarios de la red deberían utilizar programas clientes que puedan trabajar con un Proxy. Los diseñadores han creado muchos protocolos TCP/IP. Como http, FTP y otros pensando en la posibilidad de utilizar un Proxy.

En la mayoría de los exploradores Web, los usuarios pueden establecer fácilmente sus preferencias de configurar para seleccionar el servidor Proxy.

Firewall a Nivel Circuito

Servidores Proxy pero en este caso el servidor establece un circuito virtual entre el usuario y el ordenador remoto que hace transparente la existencia de dicho Proxy.

Antes de determinar que clasificación se adaptan mejor ha su entrono, examine el flujo de tráfico que se puede ejercer en el entorno la mayor parte de control esta basado en una combinación de las siguientes características:

- Sentido de l trafico
- Origen del trafico
- Dirección IP
- Numero de puerto
- Autentificación
- Contendido de la aplicación

7.2 TIPOS DE FIREWALL BASADOS EN SU IMPLEMENTACIÓN

El firewall se utiliza para proteger la red interna de Internet que es pública y poco segura. Los firewall se pueden implementar utilizando hardware o software, un firewall de software es un conjunto de programas en el Gateway que monitorea todo el trafico que influye hacia y desde una red se implementan utilizando routers configurados de forma especifica. Toda la información debe atravesar el firewall y se debe verificar comprándola con un conjunto de normas específicas. Si la información

no cumple con las normas especificas, los datos se devuelven y no pueden continuar su camino hasta que cumplan con los estándares establecidos.

Un ejemplo de firewall de hardware consiste en utilizar dispositivos configurados de forma específica para controlar el tráfico entrante y saliente o simplemente una computadora que actué como firewall.

Los firewall se ofrecen en dos formas: hardware (externo) y software (interno). Ambos tienen sus ventajas y desventajas, la decisión de usar un firewall es mucho más importante que la decisión de cual tipo usa.

- Software, algunas sistemas operativos incluyen un firewall incorporados; si lo tiene el tuyo, considere habitarlo para agregar otra capa de protección aun si tiene un firewall. Si no tiene un firewall relativamente pequeño o ningún costo en algunas tiendas de computadoras, vendedoras de software. Debido a los riesgos asociados con la descarga de software de Internet en una computadora sin protección.

- Lo mejor s instalar el firewall de un Cd, Dvd o disco flexible. Aunque confiar solo en una firewall de software proporciona un poco de protección, hay que reconocer que tener el firewall en la misma computadora que la información que tratas de de proteger puede impedir la habilidad de los firewall de atrapar trafico malicioso antes de que los firewall de atrapar trafico malicioso de que este entre al sistema.

- Hardware, típicamente llamado firewall de red, estos dispositivos externos se colocan entre la computadora o red y el modem de cable o Dsl. Muchos fabricantes y algunos proveedores de servicio de Internet ofrecen dispositivos llamados “ruteador” que también incluyen características de firewall. Los firewall basados en hardware son particularmente útiles para proteger varias computadoras pero también ofrecen un alto grado de protección para una sola computadora. Si solo tiene una computadora detrás del firewall, o si estos seguros que todas las otras computadoras en la red están actualizadas en parche, están libres de virus, gusanos u otro código malicioso, podrías no necesitar la protección extra de un firewall de software. Los firewall basados en hardware tienen la ventaja de ser dispositivos tienen la ventaja de ser dispositivos separados que controlan sus propias sistemas operativos, así que proporcionan una línea de defensa contra ataques.

Como saber que configuraciones aplicar

La mayoría de los firewall comercialmente disponibles basados tanto en hardware y software, vienen configurados de una manera aceptable segura para la mayoría de los usuarios. Como cada firewall es diferente, necesitas leer y entender la documentación que viene con este a fin de determinar si la configuración original de tu firewall es suficiente para tus necesidades. La asistencia

adicional puede ser proporcionada por arte del proveedor del firewall o de soporte técnico de un sitio Web.

Además, las alertas sobre virus y gusanos actuales como alertas de seguridad informático en ocasiones incluyen información sobre las restricciones que se pueden implementar a través de su firewall. Desafortudamente, aunque los firewall correctamente configuradas pueden ser eficaces en el bloqueo de algunos ataques, no debe caerse en una falsa sensación de seguridad.

Aunque ofrezcan realmente una cierta cantidad de protección, los firewall no garantizan que su computadora no será atacada. En particular, un firewall ofrece poca o ninguna protección contra virus que trabajan haciendo que el usuario ejecute el programa infectado en su computadora, como muchos virus de correo lo hacen.

Sin embargo, usando un firewall junto con otras medidas de protección (como software antivirus practicas seguras de computo) reforzando su resistencia a ataques) reforzando su resistencia a ataques.

7.3 Los Firewall Ofrecen un Escenario Defensivo

Los enrutadores tienden a crear una visión amistosa del mundo. Se centran en las direcciones y las mejoras rutas para entregar a estas direcciones. Por el contrario, los Firewall tienen una visión militarista de las cosas, donde las direcciones todavía son importantes, pero para inspeccionar y autorizar en lugar de entregar.

Los firewall define el mundo como el interior de la red, donde la división se hace de acuerdo a que esta mas allá del perímetro de seguridad. El perímetro de seguridad en sí se establece por uno o más firewall colocados entre la red asegurada y el exterior. Los firewall clasifican cada red que encuentra en una de las 3 categorías siguientes:

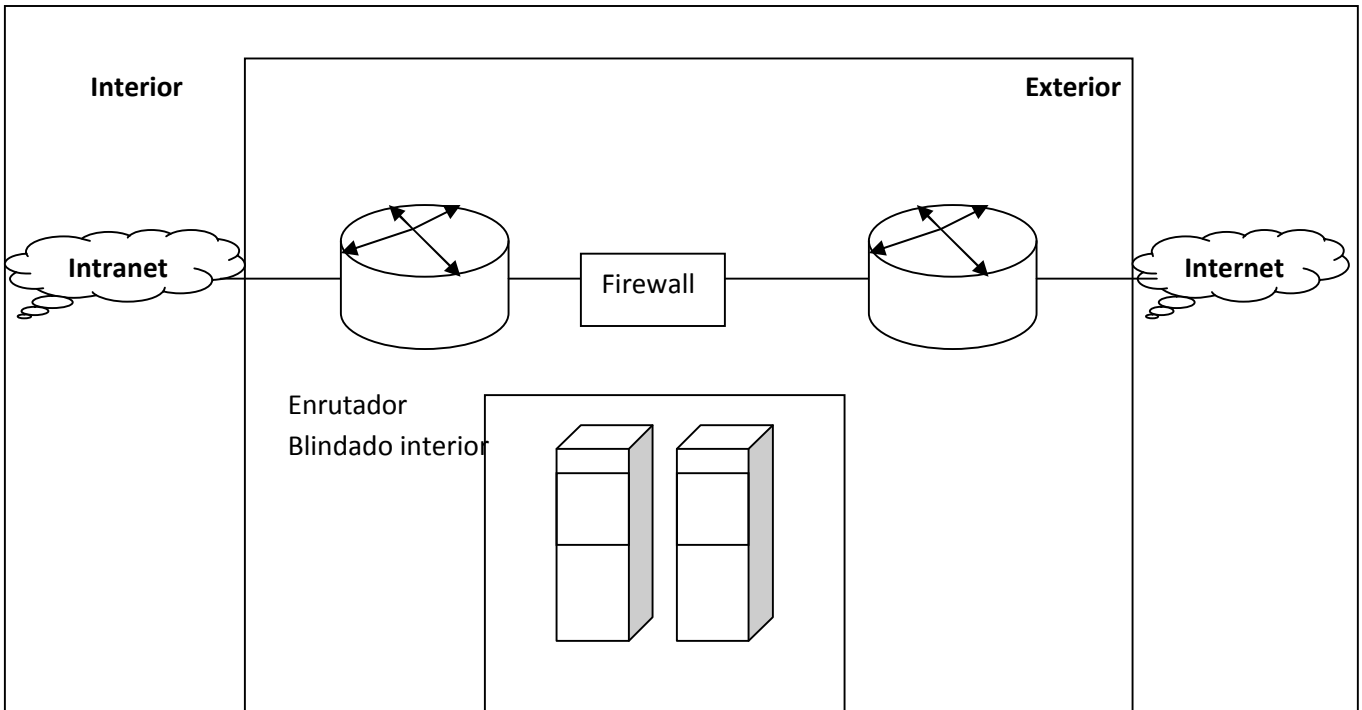
- **Red segura:** Dentro del perímetro de seguridad y baja total control administrativa de la entidad u organizada.
- **Red no segura:** Fuera del perímetro de seguridad y conocida para los firewall, pero fuera del control administrativo de la empresa.
- **Red desconocida:** De los que los firewall no han recibido información o instrucciones, básicamente casi todos de internet.

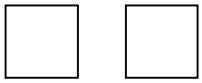
El perímetro de seguridad se traza el mismo centro del firewall, donde la propia configuración física del dispositivo define lo que es interno y lo que es externo. Las interfaces interiores y exteriores. La red conecta a cada interfaz se designa alternativamente como red exterior.

En términos de seguridad de red, el control administrativo es la posibilidad de hacer cosas como asignar direcciones IP, definir cuentas de usuario y contraseñas y mantener los archivos de configuración de dispositivos de la red. Normalmente, los medios de red, redes de área local (LAN) y las (WAN), sobre los que funciona una red segura son propiedad y están controlados por la entidad. La principal excepción a esto es la VPN que funciona principalmente sobre segmentos de red intermedios operados por alguien, mas pero se consideran redes seguras.

La seguridad es una cuestión de política, no de tecnología. La seguridad de redes no es solo una cuestión de cuanto control se puede ejercer, sino también de se decide ejercer. Parecido al equilibrio entre seguridad y rendimiento, también existe un equilibrio entre seguridad y conectividad. En teoría cualquier LAN puede tener una seguridad impenetrable, simplemente desconectada todos los enrutadores, conmutadores y módems que se dirigen al exterior.

Pero las empresas están obligadas a conectarse con el exterior porque las ventajas de la conectividad compensan el riesgo que esta implica. De hecho casi todas las empresas están actualmente conectadas a las más desconocidas y peligrosas redes públicas de todas. Cada vez que se conecta un sitio web de una organización para buscar información, descarga software o hacer un pedido, dicha organización asume un riesgo calculado permitiéndole acceder a alguna parte de sus sistemas. La mayoría de las empresas necesitan abrir sus redes al público, por lo menos en algún grado. Los negocios lo hacen para vender y ofrecer soporte, los gobiernos para ofrecer y las organizaciones educativas para enseñar. Los firewall intentan ayudar a equilibrar este compromiso de seguridad deliberando, definiendo un terreno intermedio llamado Zona Desmilitarizada o DMZ de forma abreviada. La figura 3.6 muestra una configuración de DMZ típica.





Servidor WEB

Servidor FTP

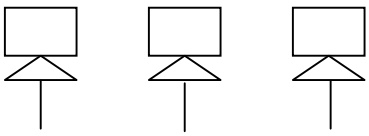
Figura 3.6 Configuración de Firewall incluye DMZ para soportar los servidores públicos

Los segmentos LAN en el exterior del firewall reciben el nombre de redes del perímetro, y las que están en el interior se llaman redes del perímetro interno. Normalmente, cada red de perímetro tiene

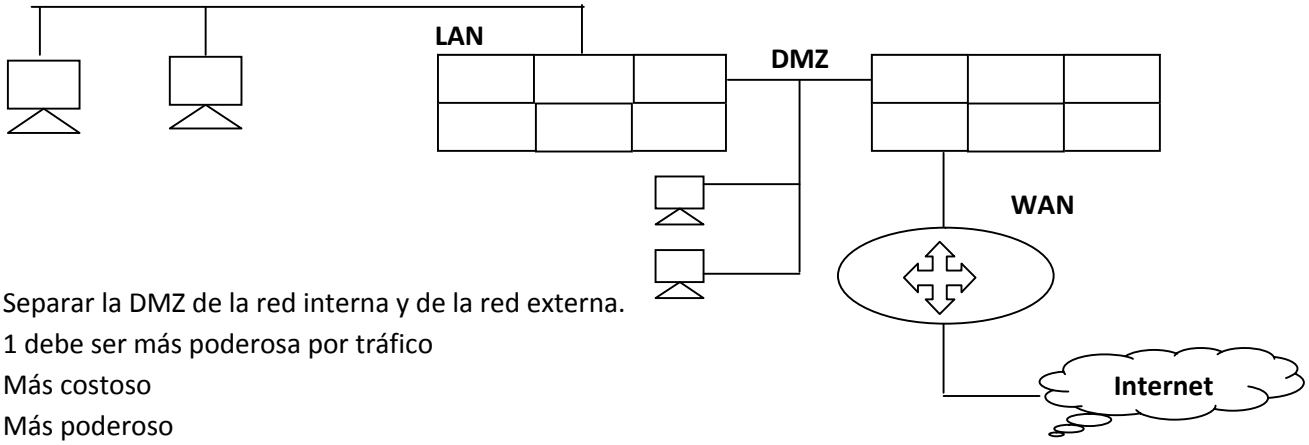
El enrutador exterior se suele llamar enrutador blindado, que normalmente tiene un proveedor de servicio de internet conectado al menos a una de sus interfaces. Además de las tareas conectadas al menos a una de sus interfaces. Además de las tareas normales del enrutador blindado también protege a los servicios de la DMZ de los ataques, actuando como un sistema de alarma para el firewall. El enrutador interior, llamando el enrutador blindado interior, es la última línea de defensa entre los firewall y las redes interiores. El punto clave que debe comprender es que el firewall está definido tanto por su configuración física (que está conectada a que) como por las reglas de seguridad que está programado para hacer cumplir.

Zona Desmilitarizada

Un firewall sirve para impedir que un atacante pase de una red a otra. Es el caso típico un firewall se sitúa entre un red no fiable y una red interna. Actualmente más y mas empresas colocan también un firewall interno. Por ejemplo entre el departamento de nominas y el resto de la organización.



- El 1 debe permitir el tráfico al DMZ y del DMZ hacia fuera
- El 2 debe permitir únicamente el trafico saliente a Internet



Separar la DMZ de la red interna y de la red externa.
1 debe ser más poderosa por tráfico
Más costoso
Más poderoso
Más complejo de administrar.

Figura 3.7 Zona Desmilitarizada

CAPITULO 8

FIREWALL PIX

Las reglas de seguridad se definen para cada interfaz de red de los firewall. Esto es así en los firewall es un enrutador que intenta hacer que las funciones de firewall y de dispositivos de alta tecnología dedicada, como el cortafuego Pix de Cisco.

Todos los paquetes se filtran basándose en las reglas que se aplican a la tarjeta de interfaz de red específica mediante la que se accedió al firewall. El hecho de configurar un cortafuego, entonces es en gran parte una cuestión de asignar reglas de seguridad a cada interfaz del cortafuego.

La lista de acceso es la herramienta más básica de seguridad de redes. La forma más sencilla de tecnología de seguridad de red es la lista de acceso. También llamadas listas de control de acceso a filtros, la lista de acceso es un componente básico de cualquier configuración de enrutador. Como el nombre índice, las listas de acceso restringen en tráfico al que se le permite acceder a una red. Las listas de acceso ofrecen un nivel básico de seguridad de red filtrado los paquetes de acuerdo a tres criterios.

- **Direcciones IP:** La dirección IP desee la que se origino el paquete.
- **Dirección Destino:** La dirección IP (o direcciones) a la que se dirige el paquete.
- **Numero de Puerto:** El protocolo del nivel aplicación (nivel7) que usara el paquete.

Cisco llama a estas líneas de acceso extendidos, donde la extensión es el numero de puerto. Los primeros productos de Cisco usaban solo direcciones origen –destino que se conocían con el nombre de listas de acceso estándar. Pero no se engañe por esta terminología; las listas de acceso extendidas son el tipo básico de lista de 3 acceso que están usando ahora.

Los números de puerto (también llamados puertos de redes), simplemente puertos) no son los puertos de interfaz físicos como sistemas operativos. Los mensajes enviados usando los protocolos de la capa de transporte TCP (nivel 4) usan número de puerto para identificar el protocolo de aplicación que realiza la transmisión. Por ejemplo, el numero para HTPP (www) es el puerto 80, es el Smtp es el puerto 25 y el FTP es el puerto 21.

Los administradores de red crean listas de acceso en el archivo de configuraciones del enrutador, se crean una lista de acceso para cada interfaz de red. Si una interfaz maneja tráfico en varios protocolos de red, por ejemplo IP,IPX y APPLE , cada protocolo de red tiene su propia formato de lista de acceso. Por tanto, debe crearse una lista de acceso independiente para ejecutarlas sobre dicha interfaz de red. Si no se tiene en cuenta el protocolo de red usando, cada criterio (reglas de acceso) ocupa una línea en la lista. Usa un enrutador que restringe el flujo entre departamentos dentro de una organización.

A medida que cada paquete intenta entrar a una interfaz, se examina su cabecera para ver si todo coincide con la lista de acceso. El enrutador está buscando coincidencias positivas. Cuando encuentra unas coincidencias no se realizan más evaluaciones. Si la regla coincidentes una regla permitir el paquete se reenvié al exterior a una interfaz de red al otro lado del enrutador. Si la regla coincide es una regla denegar, el paquete se desecha en la propia interfaz de red al otro lado del enrutador. Si la regla coincide es una regla denegar, el paquete se desecha en al propia interfaz.

Si se realiza una evaluación del paquete hasta llegar al final de la lista de acceso sin encontrar una coincidencia, se desecha de forma predeterminada. Este mecanismo se llama regla de denegación implícita, que proporciona una medida añadida de seguridad al manejo coincidencias no anticipadas en la lista de acceso.

El enrutador evalúa el paquete una regla cada vez, desde la línea superior hasta la inferior. Tengo en cuenta que este ejemplo es para IP u la sintaxis varia ligeramente para IPX, APPLE y otros protocolos es de red no IP.

Una lista de accesos coherentes se crea usando un nombre de lista de acceso al principio de cada sentencia para una lista de acceso IP. Cada sentencia debe declarar un protocolo de transporte: La transmisión control de protocolo (TCP) o el internet control de protocolo de mensajes si la regla implica una aplicación de re, la sentencia debe declarar primero un protocolo de transporte con el protocolo de aplicación.

La lista de acceso se activa en una interfaz con el comando Access-group, como se muestra en el siguiente fragmento de código. La primera línea <<apunta>> al IOS en la interfaz seria 10, línea aplica la lista de acceso 100 a todo el tráfico entrante que intente entrar a través de serial 10.

Myrouter (config)# interface serial 10

Myrouter (config) #tcp acces-group 100 in

Los enrutadores buscan coincidencias entre el contenido de la cabecera del paquete y la lista de acceso de la interfaz. Una parada seria una dirección destino o número de puerto. Si la regla coincide es una regla permitir, el paquete se reenvía. Sin embargo, sin coincidencias con una regla, el paquete se descarga sin evaluar las reglas restantes de la lista.

Una lista de acceso puede tantas reglas de filtrado como se desee, siendo el límite practico la cantidad de memoria del enrutador que requiera usar filtrado de seguridad en vez de usarla para enrutamiento. Como reglas de la lista de acceso se evalúan de arriba abajo, las coincidencias que se encuentran más frecuentemente deben colocarse en la parte superior de la lista para no desperdiciar ciclos de CPU.

Tenga en cuenta que una lista de acceso, por si sola, no convierte en una enrutador en un cortafuego. La mayoría de las listas de acceso estándar se usan para administrar tráfico básico dentro de las redes. Sin embargo, es posible configurar físicamente un enrutador como un punto de contención de de forma que todo el trafico debe pasar por una lista de acceso, convirtiéndolo así en un firewall sencillo. Esto se suele hacer para restringir el acceso entre redes que forma una red mayor. De hecho, el ISO estándar tiene docenas de comandos orientados a seguridad, además del comando acceso- list, que también se usan en los firewall de CISCO. Pero basarse en la lista de acceso como pieza central de una configuración de firewall implicaría obtener una seguridad cuestionable.

Las litas de acceso crean pasarelas de seguridad pésima porque son sin estado. Sin embargo significa que las reglas de acceso se aplican sin la ventaja se comprende el contexto de cada conexión realizada entre los equipos (llamando sesiones). Los filtros sencillos de paquete no saben en absoluto a que sesión pertenecen los paquetes, por lo que las decisiones de reenviar o desechar los paquetes se basan estrictamente en la dirección origen, la dirección destino o el numero de puerto. Saber a qué conversación pertenece un paquete mejorar la seguridad.

8.1 LOS FIREWALL HACEN UN SEGUIMIENTO DE LAS SECCIONES DE LAS REDES

La tecnología de firewall crea lista de acceso haciendo un seguimiento de las sesiones. Esta tecnología se conoce con el nombre de filtrado de paquete de estado o basado en el contexto,

porque es posible manejar un paquete individual basándose en el contexto más grande de su conexión. Este tipo d filtrado usa lo que algunos llaman listas de acceso reflexivas, que reciben este nombre porque su contenido cambia dinámicamente en respuesta reflexiva al estado de las sesiones individuales (si la sesión se inicio desde un equipo interno, cuando tiempo lleva ejecutándose) la figura 8.1 muestra como hace un seguimiento de las sesiones un firewall basado en contexto. TCP y UDS son protocolos que se ejecutan en la capa de transporte (Nivel 4) del modelo de referencia OSI de siete capas TCP es el acrónimo de protocolo de control de terminal un protocolo orientado a la conexión diseñada para soportar comunicaciones Full-Duplex con entrega garantizada. La gran cantidad de trafico IP se realiza mediante conexiones, sin extras, de bajas sobrecargas, que no garantizan la entrega ni la corrección de errores. UDP lo usan las aplicaciones relativamente sencillas y no critica como TFTP (Protocolos Trival de Transferencia de Archivos). Un tercer protocolo de trasporte es ICMP (Protocolo de internet de control de mensajería) un protocolo especializado ping y traceroute.

Un firewall realiza el seguimiento de sesiones UDP, si se tiene en cuenta que UDP es un protocolo de transporte sin conexiones, que carece del establecimiento de la conexión y de las confirmaciones de TC. El filtrado UDP funciona anotando el origen/destino y el número de puerto de la sesión, y suponiendo luego que todos los paquetes que comparten estas tres características pertenecen a la misma sesión.

Sesiones UDP(normalmente una fracción del tiempo máximo establecido para las sesiones TCP) , los firewall casi siempre realizan la elección correcta.

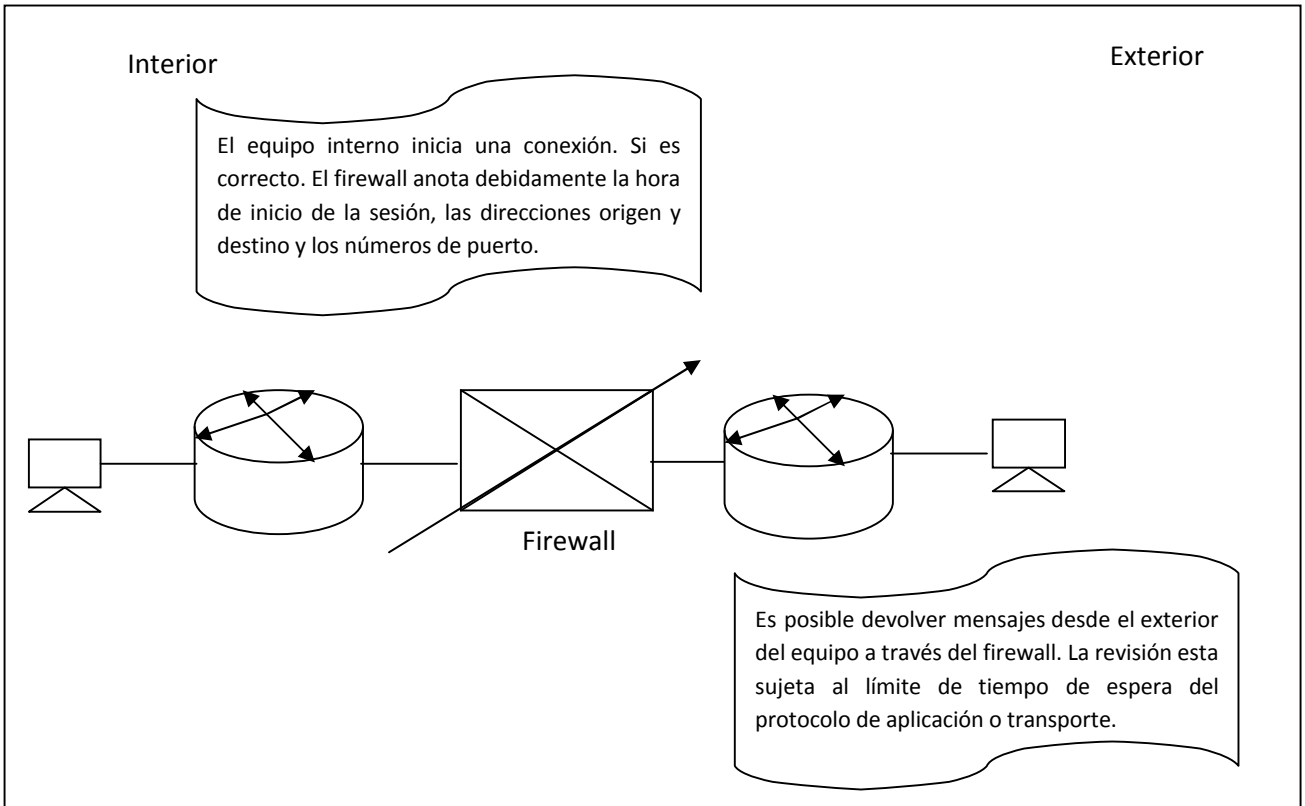


Figura 3.8 Los firewall hacen seguimiento del estado de las conexiones

Como usar Direcciones Globales para ocultar la Topología Interna de la Red.

El software IOS de Cisco tiene una capacidad llamada NAT (Direcciones de Red) que usan los enrutadores y los firewall enmascarar las direcciones de la red interna al mundo exterior. La IP permite el uso de direcciones privadas en lugar de direcciones IP registradas por ejemplo 10.1.13.en vez de 209.78.124.12, esto se hace por varias razones pero principalmente para ahorrar direcciones (a veces también espacio de direcciones) ya que simplemente no hay suficiente direcciones IP para enumerar particularmente todos los equipos, dispositivos y LAN en la mayoría de las redes. Es posible hacer funcionar una red sin direcciones privadas raramente se hace. A medida que se reenvía los paquetes al exterior, NAT sobrescribe la dirección de red interna en el campo de direcciones origen con un una dirección IP completa. Esto se hace desde un conjunto de direcciones IP registradas que se han puesto a disposiciones de NAT, asigna las direcciones locales internas al conjunto de direcciones, elimina la asignación cuando la conexión saliente que se produce, se puede ver que la traducción de NAT se realiza de una en una por tanto aunque NAT oculta direcciones interna, no conserva el espacio de direcciones.

La parte inferior de la figura muestra que NAT también puede configurarse para usarse solo una dirección registrada para todos los equipos internos con conexiones salientes. Esta función se conoce con el nombre de PAT (Direcciones de Puerto) que se difiere de NAT por traducir a una dirección externa global en lugar de la dirección externa individuales. Las direcciones de puerto ofrecen seguridad adicional haciendo imposible que los hackers identifiquen equipos individuales dentro de una red privada porque todo el mundo aparece como proveniente de la misma dirección de equipo. Además de mejorar la seguridad PAT, también conserva el espacio de direcciones.

La traducción de direcciones es un ejemplo de la importancia de hacer un seguimiento de la sesión basada en el contexto. Sin la posibilidad de hacer un seguimiento de la sesión a la que pertenece cada paquete, no sería posible asignar direcciones internas de forma dinámica a las direcciones púbicas.

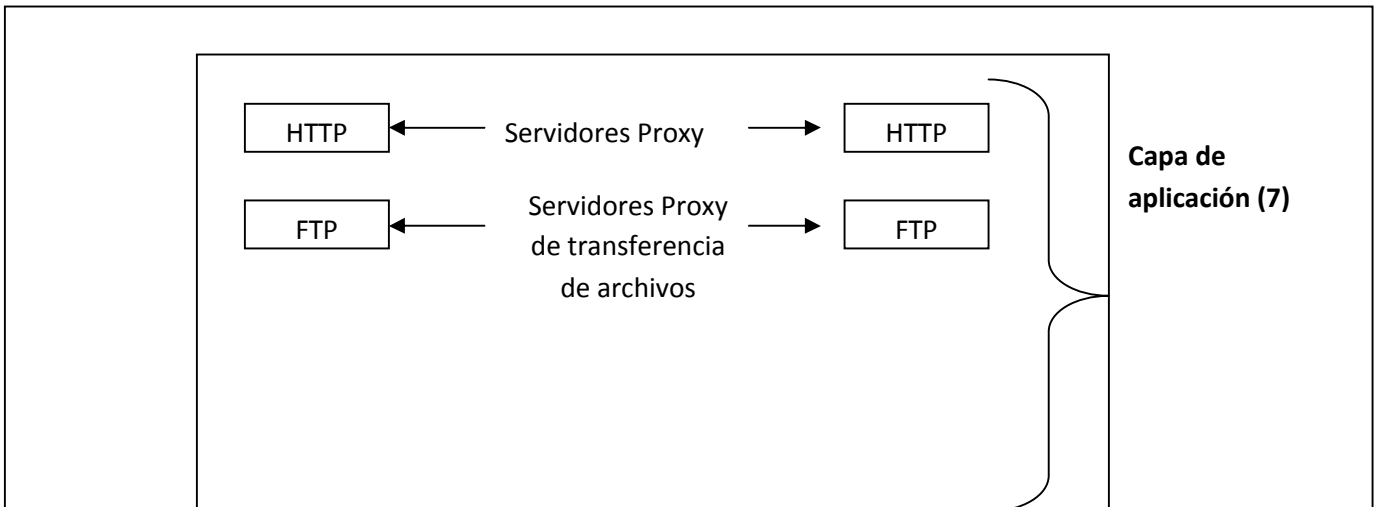
8.2 SERVIDORES PROXY

Un servidor proxy es una aplicación que actúa como intermediario entre dos sistemas finales. Los servidores Proxy funcionan en la capa de aplicación (nivel 7) de los firewall, donde se obliga a los extremos de una conexión a canalizar la sesión a través del Proxy. Esto se realiza creando y ejecutando un proceso en los firewall que crea una imagen espejo de un servicio como si estuviera ejecutándose en todos los equipos finales. Un servidor Proxy esencialmente convierte una sesión de dos partes en una sesión de cuatros partes, donde los procesos intermedios emulan los dos equipos reales. Como operan en el nivel 7, los servidores Proxy también se conoce con el nombre de firewall de la capa de aplicación.

Es necesario ejecutar un servidor Proxy por cada tipo de aplicación de internet que soportan los firewall, un firewall, un proxy de SMTP para el correo electrónico, un proxy de SMTP para el correo electrónico, un proxy de http para servicios web. Los servidores Proxy son casi siempre equipos de una dirección que van a desde la red interna a redes externas. En otras palabras si un usuario interno quiere acceder un sitio web en internet, los paquetes que forman esa petición se procesan a través del servidor HTPP antes de reenviarse al sitio web. Los paquetes devueltos desde el sitio web se procesan a través del servidor http antes de direcciones al equipo interno del usuario. Al igual que con la NAT, los paquetes van al servidor web externo transportando la dirección IP del servidor http en vez de la dirección interna del equipo.

Como los servidores Proxy centralizan toda la actividad para una aplicación en un solo servidor, estos presentan la oportunidad ideal de realizar funciones útiles, tener la aplicación ejecutándose justo delante de los firewall ofrece la oportunidad de inspeccionar los paquetes para buscar más cosas que las direcciones origen-destino y los números de puerto. Esta es la razón por la que prácticamente todos los firewall modernos incorporar laguna forma de arquitectura de servidor proxy. Por ejemplo los paquetes que llegan a dirigidos a un servidor configurado estrictamente para ofrecer información (un servidor FTP) pueden inspeccionar para ver si contiene algún comando de escritura, de esta forma el servidor proxy puede permitir solo conexiones que contengan los comandos de lectura.

El servidor Proxy es otra tecnología posible solo en firewall basados en el contexto. Por ejemplo si un firewall soporta miles de conexiones web simultáneas, debe pos supuesto ordenarlas para saber a qué sesión pertenece cada una de los millones de paquete entrantes con el número de puerto 80 (http).



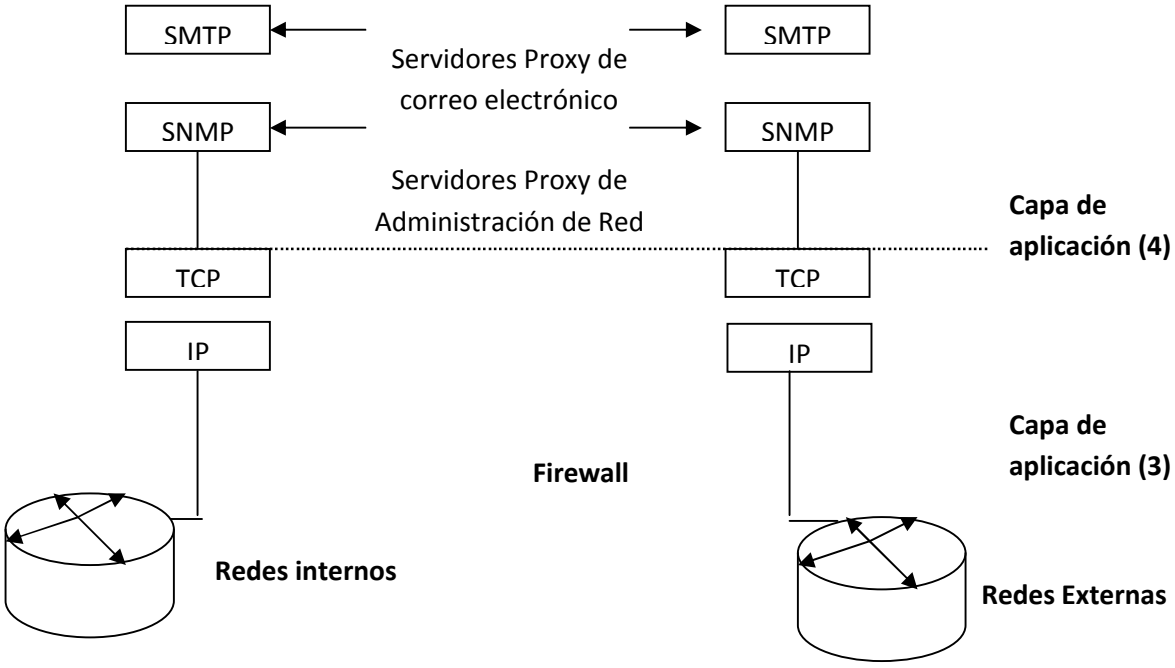


Figura 3.9 La Tecnología de servidor Proxy es la base de los firewall avanzados

8.3 FIREWALL PIX DE CISCO (HARDWARE)

El firewall PIX es un dispositivo de hardware que actúa de firewall y es capaz de proteger redes de tamaños muy diversos, desde pequeños oficinas hasta empresas.

Es esencia PIX firewall es simplemente una PC forzada con un programa de firewall le permite ser competitivo en precio, al tiempo que la imagen del software especializado que tiene instalado hace posible que este evento de debilidades de seguridad que son comunes a las soluciones de firewall que funcionan en los más conocidos sistemas operativos de uso comercialmente. Pix firewall incluye una serie de características concebidas con el fin de asegurar la red frente a la mayoría de amenazas posible.

La principal de estas características se conoce como el algoritmo de seguridad, ya que permite el establecimiento de conexiones desde adentro y denegar los intentos de conexiones desde el mundo exterior de forma dinámica.

El firewall Pix soporta también funcionamiento en reserva permanente con lo que se usan firewall pix redundantes que se elevan unos a otros en caso de fallo son interrumpir el servicio al usuario.

El firewall pix es un paquete preparado para competir con otros firewall que existen en el mercado ya que el firewall pix posee:

- **Hardware/ Software Integrado:** El firewall Pix es un paquete integrado en una plataforma hardware construida a propósito para ofrecer servicios intensivos de firewall. No se incluye como un paquete software independiente.
- **Adative Seuritu Adgorithm:** No es ni un filtro de un firewall de aplicación Proxy. Pix implementa una arquitectura que ofrece alto rendimiento disminuyendo el uso del Proxy.
- **Opcion Vpn Integrada:** Una tarjeta complemento de procesador configura redes privadas virtuales que soportan el cifrado avanzado y los estándares de intercambio de claves de internet.

Los administradores de red cada vez usan más dispositivos construidos a propósito, como firewall pix de Cisco, para cubrir sus necesidades de seguridad de red. El sistema electrónico y el software del firewall pix están ajustados específicamente para equilibrar la funcionalidad de seguridad avanzada con la necesidad de un alto rendimiento. El cortafuego pix y los productos que son dedicados como el, tienen el nombre de equipos de red, el nuevo término que está de moda para estos dispositivos ya que estos tienen la funcionalidad de las redes muy claramente definida.

Se dice que cisco esta hacienda del firewall Pix un sistema incrustado de tiempo real frente a los equipos firewall de los competidores basados en plataforma UNIX. Se argumenta que los firewall basados en equipos de UNIX deben de pagar un precio tanto de rendimiento, como en seguridad. El núcleo de un sistemas operativo de propósito general como lo UNIX no solo tiene las latencias, sino también cuenta con sobrecargas inadecuadas para las tareas de los firewall, además de que cuenta con agujeros de seguridad que los hackers pueden usar para introducir el firewall.

8.3.1 EL ALGORITMO DE SEGURIDAD ADAPTATIVO (ASA) DEL FIREWALL PIX

Un esquema de protección basado en ASA tiene en cuenta las direcciones origen y destino, los números de secuencia TCP, numero de puerto y banderas TCP adicionales. Es decir, el esquema ASA ofrece seguridad basada en el estado y orientado a conexión, toda la información de los paquetes se almacena en una tabla. Todo el trafico entrante y saliente se compara con las entradas de esta tabla para detectar y trafico erróneo, no deseado o con problemas con la seguridad o el enrutamiento.

Un algoritmo no es nada más que un conjunto de reglas ordenadas con cuidado y que se aplican de forma muy rigurosa de un proceso repetitiva y con la capacidad de manejar condiciones variables de un forma lógica un ejemplo de ello son las computadoras que hacen el uso intensivo de los algoritmos ya que debido a que en la informática todos es repetitivo y manipulador por variables.

Pero ASA tiene un conjunto de comandos, que son específicos de los firewall. ASA permite al firewall PIX implementa unas medidas de seguridad más estrictas y escalarse a pasarelas de mayor tamaño. La tendencia de la seguridad de las redes es potente, y la posibilidad de designar redes y equipos con un gran espectro de niveles de seguridad, en vez de un simplemente <fuera> y <dentro>.

El comando name if (nombre de interfaz) de FIREWALL PIX le deja especificar los niveles de seguridad relativos para cada interfaz, tanto dentro como fuera de los firewall. El aplicar los niveles de seguridad relativos, de interfaz por interfaz, da la posibilidad de dibujar un mapa descriptivo del que sería capaz definiendo todas las redes como dentro como fuera.

El usuario debe introducir el comando nameif para cada interfaz. Puede elegir cualquier valor para un nivel de seguridad entre 0 y 99, y dos interfaces en un firewall PIX no pueden tener el mismo nivel, la práctica común es asignar niveles de decenas, como se muestra el siguiente fragmento de código. 8 interfaces en tres zonas de seguridad.

Firewall (config)# nameif etherne0 outside security 0

Firewall (config)# nameif etherne0 outside security 10

Firewall (config)# nameif etherne serial outside security 20

La forma que tiene de funcionar los niveles de seguridad es que cada equipo de una red toma el nivel de seguridad que se asigna. Una conexión que se realiza desde un nivel superior a otra red de menor nivel, el software la trata como externa; una dirigida desde un interfaz de menor nivel a otra de un nivel superior se trata como interna. Este esquema permite al administrador de red aplicar reglas de forma mucho más granular.

Cada zona tiene su propia seca de seguridad, existe la posibilidad de implementar comprobaciones de seguridad entre zonas. Por ejemplo, las listas de acceso pueden aplicar restricciones en el tráfico que fluye entre equipos conectados a las dos redes DMZ.

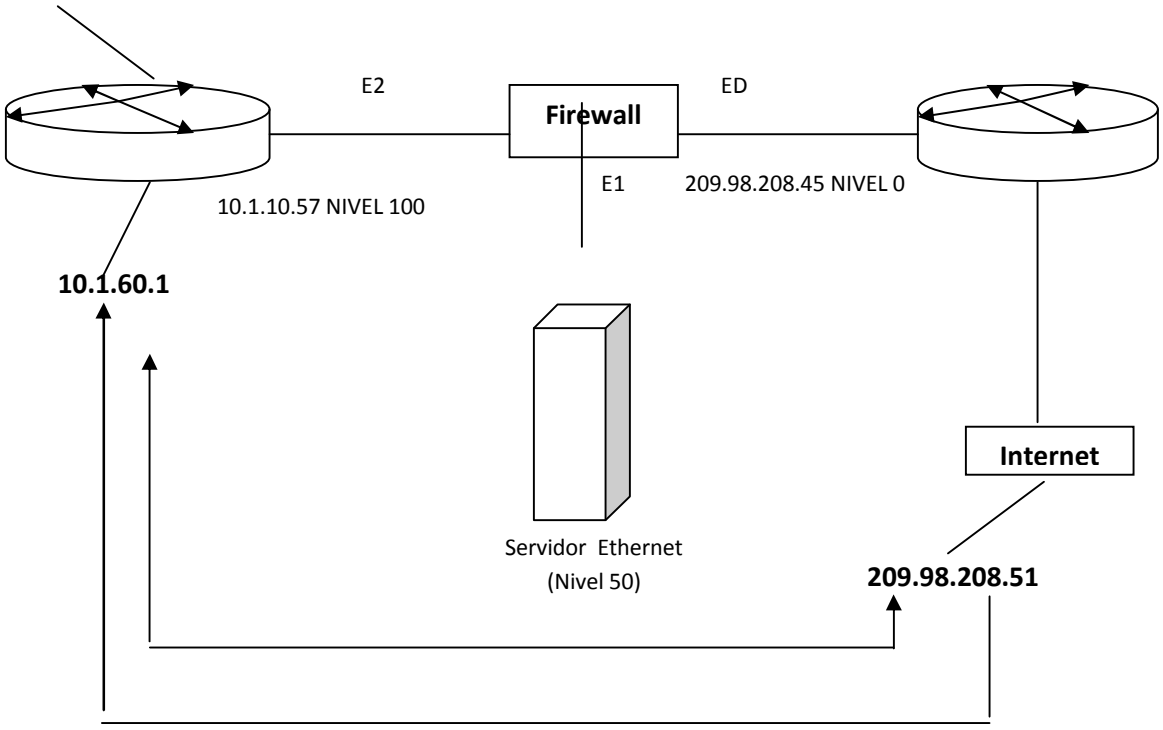


Figura 4.0

8.3.2 RANURAS DE TRADUCCIÓN DEL FIREWALL PIX

La traducción de direcciones y el seguimiento de sesiones con la parte central de la arquitectura. Pero los sistemas Pix usan sistemas más formales para implementar la traducción de direcciones IP. ASA asigna una ranura a la nueva conexión. Los firewall PIX se venden con licencias de conexión que limitan al número total de conexiones que pueden usarse simultáneamente. Cada sesión consume una ranura. Las ranuras configuradas, tanto con el comando global como con el comando static se conocen a veces con el nombre de xlates, aunque estas se llaman normalmente ranuras. Cuando se inicia la conexión, ASA toma una ranura del grupo de licencias e introducción la sesión en la tabla de estado. La ranura se devuelve al conjunto cuando la sesión finaliza.

Si una red necesita más conexiones simultaneas que licencias tiene, el operador donde puede comprar una licencia de software mayor de cisco. La tabla 1 muestra los incrementos en que se pueden licenciar las ranuras del firewall PIX.

Para ayudar al administración de consumo de ranuras, se puede especificar un límite de ranuras cuando este configurado interface con el comando NAT. De esta forma, los administradores de red pueden evitar que los usuarios de red individual consuman demasiadas ranuras de traducción. El número de conexiones simultáneas está en función de la memoria de firewall.

Algunas de las aplicaciones usan más de una conexión a LA vez uno de los ejemplos es que FTP utiliza dos conexiones. Un explorador WEB (que ejecuta el protocolo HTTP) hasta cuatro o más conexiones, dependiendo de si esta en el proceso de carga de una página o algún otro objeto como los subprogramas java. No debe pensar en las conexiones de internet en términos de algo que el usuario consiste decide en iniciar y detener. Las sesiones se inician y se cierran sin nuestro conocimiento, por ahí se dice que Microsoft internet Explorer consume hasta 20 conexiones TCP por usuario.

8.4 CONFIGURACIÓN DE FIREWALL PIX

Ahí examinaremos una conexión sencilla de firewall Pix como de algunos comandos que nos ayudaran a comprender las operaciones básicas del firewall Pix. La configuración Pix de tres interfaces con un enrutador blindado interno o un servidor DMZ conectado. La configuración incorporación traducción de direcciones global, restricciones sobre el trafico exterior y la ruta estática exterior con un conducto interno.

El primer paso consiste en entrar al modo para configurar la interfaz, apuntando a cada interfaz conforme se esta configurando:

Firewall>enable

Password: ****

Firewall # config t

Luego, se usan los comandos interfase para designar las zonas de seguridad y noveles de las interfaces:

Firewall (config)# name if Ethernet0 outside security0

Firewall (config))# name if ethernet0 extranet security50

Firewall (config)# name if Ethernet0 inside security100

A continuación los comandos interfase definen la especificación Ethernet que funcionan sobre las interfaces (auto sensibilidad 10/100 Mbps):

Firewall (config) #name if Ethernet0 auto

Firewall (config) #name if Ethernet1 auto

Firewall (config)#name if Ethernet2 auto.

Las interfaces deben identificarse con las direcciones y mascaras IP, lo que se hace usando los comandos IP dress. Tenga en cuenta que se usan nombre que ha asignado a la interfaz (outsider, extranet e inside), se usan las direcciones IP Internet privadas para la interfaces extranet e incide (100.1.5.2 y 10.1.10.57):

Firewall (config) # ip address outsider 209.98.208.45 255.255.255.240

Firewall (config) # ip address extraner 10.1.5.1 255.255.255.0

Firewall (config) # ip address inside 10.1.10.57 255.255.255.0

El commando NT se usa para permitir a todos los usuarios de dos grupos de usuarios de dos grupos de usuarios internos realizar conexiones externas usando direcciones IP traducidas. El número que sigue a los argumentos (inside) de las 2 sentencias es un numero ID de NAT o numero de referencia NAT (1 y 2) que se usa para enlazar grupos a conjuntos de direcciones globales:

Firewall (config)# nat (inside) 1 10.0.0.0 255.0.0.0

Firewall (config) # nat (inside) 2 10.0.0.0 255.0.0.0

Las sentencias que se usan en el commando global crean 2 conjuntos de direcciones globales. Estas se asignan a usuarios mediante los números ID y NAT (1 y 2 aquí). La sentencia del medio es el conjunto de direcciones PAT. Lo que ocurre aquí es que al sistema se le ha indicado que asigne direcciones NAT y, cuando todas estén todas las co en uso, empiece a aplicar las direcciones globales PAT a las sesiones.

Todas las conexiones asignadas a direcciones PAT mostraran una direccion origen 1 209.98.208.50.

Firewall (config) #global (ostside) 1.2098.98.208.46 209.98.208.49 net mask 255.255.255.240

Firewall (config) #global (outside) 1.2098.98.208.50 net mask 255.255.255.40

Se usara una dirección estática para creación IP visible externamente. Una declaración counduit permite a u nequipo o red especificada

Se usara una direccion estatica para creación IP visible externamente. Una declaración **counduit** permite a un equipo o red especificada un socio de negocio, por ejemplo conectarse a traves de un firewall PIX. La siguiente declaración de ejemplos permite a los usuarios que usan un equipo externo acceder a través del firewall al servidor 10.1.60.1 mediante conexiones TCP para acceso a Web. La clausula **eq 80** especifica una conexión TCP debe estar activada (igual a) a puerto 80, el numero de

puerto para el protocolo de la aplicación http. El modificador **any** permite que cualquier equipo externo se conecta a 10.1.60.1.

Firewall (config) #**static (incide,outside) 209.98.51 10.1.60.1**

Net mask 255.255.255.0

Firewall (config) # conduit permit tcp host 10.1.60.1 eq 80 any

Esta declaración que usa el commando **outbound** crea una lista de accceso que permite a la web a un equipo interno (puerto 80), pero le impide descargar subprogramas de Java. Pix usa el comando **outbound** para crear listas de acceso y el comando **apply** para aplicarlas. Tenga en cuenta que el numero de puerto. Es posible usar nombres en lugar de numero para algunos de los protocolos mas nuevos de la capa de aplicación como Jaca. Obviamente es mas facil recordar nombres ven vez de un numero cifrado. La opcion outgoing_src deniega o permite a una dirección interna la posibilidad de iniciar conexiones externas usando los servicios especificados en el comando outbound.

Firewall (config) # outbound 10 permit 209.98.208.22 255.255.255.255 80

Firewall (config) # outbouubd 10 deny 209.98.208.22 255.255.255.255 java

Firewall (config) # apply (extranet) 10 outgoing_src

Hay otros muchos commando que se pueden usar cuando se este configurando un firewall PIX. De hecho, en la mayoria de los entornos de redes, es necesario configurar otros parámetros más para conseguir que los firewall funcionen correctamente. Tardara varios días en configurar correctamente un firewall PIX con multiples servidores, protocolos, listaa de accesos y enrutadores blindados. Las configuraciones posibles son interminables. Pero las sentecnias sencillas que hemos explicado se muestra que configurar un firewall, uno de los dispositivos de redes mas complejos no es una gran ciencia. Puede complicarse muchos, pero hacerlo es solo cuestion de hacer las cosas de interfaz en interfaz, de comandos en comando.

Hay muchos elementos importante en la configuración de los firewall, un ejemplo seria configurar 2 firewall, uno con el servidor pasarela primario y el otro como una caja de seguridad activa a al que que se desviara el trafico si el servidor primario falla.

Modelo Diferentes de Firewall PIX (Hardware)

El hardware de PIX tiene muchas configuraciones diferentes que se planea para asegurar que el producto que se quiere satisfaga en los diferentes ambientes. Obviamente, los requisitos del usuario a veces diferentes de aquellos de un proveedor de servicios. Cisco ha proporcionado varias clases con los puntos del precio diferentes para asegurar la colocación del producto óptima.

Modelo

Se apoya cinco modelos actuales: 501, 506e,515 E, 525 y 535.

Hay tres modelos que usted podría ver desplegados en la empresa sin embargo, los ambientes son: 506,515 y 520.

PIX 501

Los 501 son el modelo de la entrada básico para el PIX y tiene una configuración fija.

Tiene cuatro puesto 10/100Mbps interruptor para la conectividad interior y una sola interfaz de 10 Mbps por conectar a la Internet el dispositivo (como MODEM de cable p DSL). Proporciona 3Mbps todo poner en una 3des conexión de ipsec que debe exceder el requerimiento. La de un usuario utiliza la licencia baja en una licencia del 10-usuario con Des Ipsec; optativa es una actualizacion de los 50 usuarios y/o 3Des apoyo de VPN.

Los 501 son basados en un 133Mhz AMD el procesador de sc520 con 16 MB de ram y 8 de flas. Estos son un puerto de la consola, Rj45 medio doble 10 Bse T puerto para el exterior, y un integro, autosensing, automóvil MDIX 4 puerto RJ45 10/100.

PIX 506

Los 506 son el dispositivo de oficina de office, el dispositivo de oficina de rama. Una vez mas el aparato no es configurable del hardware, con un puerto de la consola y 2 auto negaciones, RJ45 10 baseT puerto, uno para dentro de y uno fuera de. La actuación es grandemente aumentado: los 506 apoyan 8Mbps throughput del calro texto, con 6Mbps 3 DES, Ipsec que debe permitir centenares de apoyo a usuarios de oficina de rama en un VPM. El harware es basado en un 200 MHZ

PIX 515

EL próximo paso a la balanza es el 515, internacional para el centro de la empresa o del pequeño negocio mediano. De nuevo, este producto tiene actuación de los alamabres, se maneja a 170 MBPS de claro-texto.

El chasis es una 1U caja de la pizza, internacional para la montura de la percha. Probablemente es mas la diferencia entre 506 y 515 son 1 que el chasis es configurable; viene rápidamente con una henchidura para un solo puerto adicional o cuarto puerto Ethernet unen, mientras permitiendo el

interior; fuera de y cuatro servicio adicional de re. La unidad esta basada en 200Mhz Pentium de Intel MMX con 32 MbDE RAM 8 Mb de llamarada como los 506E. la autorización es flexible para que las empresas puedan comprar lo que ellos necesitan. La licencia restringida limita el número de interfaz a tres y no apoya disponibilidad. Lo alto de la licencia sin restricción permite un aumento en el RAM (de 32 MB a 64 MB) y a seis interfaces, junto con la capacidad del fallo.

PIX 515E

Los 515E reemplazaran a los 515 en el 2008 de mayo. Tiene una superior presentación 433Mhz Intel celaron. Crecientemente la actuación del firewall baja. Otra nueva opción es la habilidad al fuera de la carga aritmética de computo de DES del OSA un especializado. La VPN acelerador tarjeta (VAC) entregando a 63Mbps 3 DES y 2000tuneles de IP sec. Autorizar es similar; la licencia restringida lo limita a tres interfaces y ningún fallo, considerando que la licencia sin restricción tiene la memora actualizada, el vac y una seis interfaces.

PIX 520

El PIX es un pájaro impar. E diseño pájaro impar. Se diseña como el alto-extremo la plataforma de PIX, con el chasis de percha-montaña de pc-estilo y una mezcla ancha de tarjeta de los medios de comunicación disponibles, el anillo de la fihca incluyendo y fibra. Como el PIX mas temprano, los 520 vienen con un DB9 el puerto de la consala y un paseo del disquete; es basado en el 200Mhz. También es raro la autorización: como los 501,520 la licencia es basado en número de usuario. Para una entrada PIX, usted compraría PIX-Conn-128 que permitiría 128 usuarios. Estos simultaneo para las actualizaciones de la licencia a 1024 usuarios ilimitados. Teniendo el paseo del disquete es especialmente conveniente, hábiles el caso de que la red baja o por la red baja o por otra parte no se requieren los servidores del inaccesibilidad TFTP.

Estos se logran los rasgos ahora a través de la dirección de la red apropiada laborando con herramientas, tal como Cisco Works o el PIX firewall gerente.

PIX 525

El 525 reemplaza el 520 en el 2001 e junio. Se diseña para la empresa grande o el proveedor de servicios de pequeño ambiente. El disquete paso al pasado, sin embargo, los 525 todavía apoyan solo o cuatro puertos 10/100ethernet rápido 4/16, ficha el multinodo FDDI pone en tarjeta pero ahora también rocoge Gigabit Ethernet.

La actuación cuenta la historia aquí; basado en el 600MHZ Pentium de Intel III, los 525 alardean 360 Mbps throughput del claro-texto y, con la tarjeta del acelerador, 70Mbps de 3DES IP Sec socavan el trafico.

Autorizar es basado en las cuentas de la interfaz y failover, como son los modelos más tempranos. La licencia restringida limitada el PIX 525 a 128 Mb de RAM y 6 interfaces.

El RAM de los choques sin restricciones al 256MB permite a 8 interfaces y, apoyos el failover. Como antes de 3D es autorización esta separada, si deseo.

PIX 535

El 535 es le modelo de la cima de la línea, conveniente para los ambientes de proveedor de servicios. La actuación es la llave: a 1 Gbps throughput del claro-texto medio un millón las conexiones simultaneas, y 7000 inicializacion/ demoler la conexión en un segundo. Con el Vac, usted puede conseguir 100Mbps 3DES throughput, con 2000 las asociaciones de seguridad simultaneas (VPN socava)

PIX NAT

¿Qué es PIX NAT?

La caracteristicas “Network Address Translation” trabaja sustituyendo o traduciendo, direcciones de host en la red interna con una “dirección global” asociada con una interfaz externa”. Esta caracteristicas protege las direcciones de los host internos de ser expuestas en otras interfaces de red.

PIX PAT

Significa “Port Address Transalation” Puede sser configurada para que nuestro rango de IPS mapee los diferentes numeros de puertos TCP a una unica IP Pat puede ser usada en combinación con NAT.

Configuración de Múltiples Interfaces.

PIX soporta múltiples interfaces perimetrales con el objetivo de proteger nuestra red. Se puede llevar a cabo conectando tres interfaces Ethernet. La primera interfaz reside en la parte externa de la red. La siguiente interfaz puede residir en lap arte DMZ donde tienes el bastion host o host públicamente accesibles ya sean WEB, FTP o mail relay. Este método es una buena forma de incrementar la política de seguridad de tu red.

Esta configuración dejara una especie de firewall con tres brazos. Puede utilizar las interfaces con token también, no tiene que limitarse a Ethernet.

Configurar el Firewall PIX con la opcion Failover

¿Qué es Failover?

Puede utilizar la capacidad de failover del pix para tener en caso de fallo una maquina en espera que lleve a cabo el trabajo del PIX que ha fallado. Para utilizar esta opción debes tener dos maquinas PIX IDENTICAS. Si la maquina primaria "muere" la maquina secundaria adquirirá transparentemente la carga. No puedes mezclar un pix 515 con un 520 para usar la capacidad de failover. Un cable denominado de failover conectado entre dos maquinas y proporcionar la señal de control de failover.

La unidad primaria utiliza la IP y la dirección MAC de la unidad secundaria. En caso de fallo, las unidades se intercambian la dirección IP y la dirección MAC para reemplazar la una a la otra en la red. La traslación IP a MAC permanece iguales así que no hay que cambiar nada en las tablas ARP.

Filtrado de contenido

Filtrado de URL y bloqueo de java

En las mayorías de las situaciones, necesitaras permitir el acceso a través del puerto 80 para que los usuarios a Internet. Es un problema mayor ya que los applet java pueden ser descargados por el acceso http. Los applet java potencialmente peligrosos.

Configuración AAA en los Firewall PIX

¿Qué es AAA?

Autentificación de quien eres.

Autorizarte es lo que debes hacer

La autentificación es valida sin autorización

La autorización no es valida sin autentificación

La contabilidad es lo que hiciste (logging)

Trucos AAA: Si te bloquea tu mismo recuerda que hay una backdoor que te permite pasar a través del puerto de la consola con el nombre de usuario y el pass Word.

Bases VPN

¿Qué es una VPN?

La VPN se crea para utilizar Internet para establecer conexiones Wan. Es posible creando un túnel encriptada y seguro. Un vez que el túnel es creado se puede utilizar para establecer una cohesión que ahora es segura.

Para poder utilizar la VPN en pix necesitas un harware adicional:

Puedes utilizar la tarjeta de aceleración (VAC) que povee alta accesibilidad, tuneling y servicios de encriptación adecuados para conexiones locales o remotas.

Este hardware especifico esta optimizada para llevar las tareas repetitivas y matemáticas necesarias para IP sec.

Descargas del trabajo a la maquina para que lo lleve a cabo la VAC no solo mejora el rendimiento sino que mantiene la fiabilidad en los 2 lados del firewall.

Perspectivas generales del producto.

La familia Firewall PIX aparece en un amplio espectro de campos, desde firewall plug 'n' play compactos y de escritorio para pequeñas oficinas o incluso para el hogar hasta firewall por los que pasan gigabits de datos en poco tiempo.

Soportan hasta 500000 conexiones simultaneas y cerca de 1.7 gigabits por segundo (Gbps) de salida total.

8.4 CARACTERÍSTICAS CLAVES Y BENEFICIOS

Seguridad: Los firewall PIX de Cisco utilizan un sistema operativo propio y especialmente diseñado para firewall que elimina el riego asociado a los sistemas operativos de uso general. Los firewall PIX incorporan la ultima tecnología en seguridad: inspección basada en el estado (stateul inspección), VPNS basadas en IP sec y L2TP/PPTP filtrado de contenidos y detención de intrusos integrada. En le núcleo de la familia de firewall PIX tenemos el algoritmo de seguridad ASA (adptive security algorithm) que mantienen asegurados perimetralmente las redes controladas por el firewall. La inspección basada en el estado, en la que se usa el diseño ASA, permite crear flujos de sesión basándose en la dirección origen y destino, números de secuencias TCP (no predecible) números de puerto y banderas TCP adicionales. Todo el trafico entrante y saliente esta controlada por la aplicación continua de las políticas de seguridad a cada entrante en la tabal de conexiones

- Rendimiento: Altamente escalable, soporta asta 10 interfaces gigabits Ethernet y 1.7 Gbps de salida total.

- Fiabilidad: El tráfico de la red puede ser redirigido automáticamente a otra unidad en espera en caso de fallo mientras se mantiene el trafico de la red gracias a una sincronización del estado entre la unidad primaria y la unidad de espera.

- Virtual Private Networking (VPN): Servicios VPN basados en IP sec y L2TP/PPTP, adecuados para acceso local y remoto, la conexión VPN basada en Triple DES (3DES) puede ampliarse hasta aproximadamente 100Mbps usando la tarjeta aceleradora para VPNS PIX (VAC),que descarga a la maquina del trabajo de encriptar/ desencriptar dejándolo a cargo de coprocesadores especializados para esta tarea.
- Network Address Transalation (NAT) y Port Addres Translation (PAT)
- Prevención de ataques de denegación de servicios.
- Administración sencilla gracias a la interfaz Web del PIX Device manager (PDM): Esta provisto de un amplio rango de interfaces Ethernet 10/100 hasta 10 Ethernet gigabits en un único firewall.

En futuras versiones de firewall PIX se esta considerando la posibilidad de añadir lista de control de acceso (ACLS) basadas en la dirección, MAC. Por el momento si se quiere, por ejemplos permitir el acceso a un usuario con un portátil, se deberán usar métodos de autentificación a nivel de usuario usando TACACS.

El ciclo de seguridad de Cisco:

- Asegurar el entorno
- Monitorizar la actividad y responder a lo que vaya sucediendo
- Probar la seguridad del entorno
- Mejorar la seguridad del entorno.

Estos pasos son un ciclo continuo que comienza una vez definida la política de seguridad de la empresa.

Existen multitud de herramientas para probar la seguridad de una red:

Herramientas gratuitas

Nmap (www.insecure.otg/nmap)

Nessus (www.nessu.org)

Whisker (http://sourceforge.net/projects/whisker)

Security (www.arc.com/sara)

Lopthcrack (www.atstake.com/research/ic)

Herramientas comerciales

Iss internet scanner (www.iss.net)

Symantec enterprise security manager (www.pentaface.com)

8.5 TECNOLOGÍA E INNOVACIÓN DE CISCO

Cisco system anuncio hoy la disponibilidad de las plataformas PIX 506E Y 515E entregan a los clientes capacidades mejoradas, diseñadas para una seguridad para una integridad optima y un buen desempeño VPN. De acuerdo con las pruebas de laboratorio interno de Cisco, los nuevos firewall PIX 506 E y 515 E de cisco ofrecen poder extra de procesamiento. La adición de aceleración VPN basada en hardware integrado en modelo de firewall PIX 515E ofrecen funcionalidad VPN de alto desempeño y simultáneamente, recursos de sistema gratuitos para otras funciones criticas de seguridad y tomar ventajas de ebussiones y competir en la economía de Internet.

8.5.1 NUEVAS MEJORAS A LA FAMILIA FIREWALL PIX DE CISCO

La plataforma Firewall PIX 506E y 515E entregaron a los clientes capacidades mejoradas, diseñadas para una seguridad para una integridad opima y un buen desempeño VPN. De acuerdo con las pruebas de laboratorio interno de Cisco, los nuevos firewall PIX 506E y 515E de Cisco ofrecen poder extra de procesamiento. La adición de aceleración VPN basada en hardware de procesamiento. La adición de aceleración VPN basada en hardware integrado en modelos de firewall PIX 515E ofrece funcionalidad VPN de alto desempeño y simultáneamente, recursos de sistema gratuitos para otras funciones criticas de seguridad.

La infraestructura de red de nuestra compañía demanda una seguridad líder en la industria y soluciones VPN para soportar los rendimientos de negocios de nuestros clientes, dijo Hill Townsend, ingeniero de red de Lokwood Grenne, líder en construcción e ingeniería. Las nuevas mejoras de los firewall PIX 506 y 515 satisfacen estos requerimientos, entregando seguridad integrada de alto desempeño y capacidades de aceleración VPN, necesarias para nuestro negocio actual.

Cisco también introdujo la versión 6.2 de un sistema operativo, entregando a los clientes nuevas mejoras significativas para redes de oficinas pequeñas y oficinas en los hogares SOHOM y de empresas mediante, junto con soportes para voz sobre IP y multimedia.

La versión 6.2 de PIX OS permite despliegues VPN escalables y nuevas funciones como PPp sirve protocolo Ethernet y mejoras en compatibilidad para proveedores de servicios en redes SOHO. El firewall PIX puede actuar ahora como clientes VPN basado en hardware. Simplificando de manera importantes la administración de los despliegues VPN a gran escala en ambientes de oficinas pequeñas y remotas. Utilizando el mismo marco VPN unificando del clientes, disponibles también en otras soluciones VPN de Cisco, el firewall PIX disminuyen significativamente la cantidad de políticas, en la medida en que los túneles VPN estén establecidos, garantizando un despliegue de acceso remoto seguro.

La nueva funcionalidad basada en LAN amplia la capacidad del firewall PIX entregando capacidades transparentes y superando la limitación de la distancia de muchos soluciones firewall de alta disponibilidad.

Para ofrecer soporte a terceros, se ampliado los servicios URL con el apoyo de N2H2, proveedor de soluciones de Internet y miembros del programa de socio s de negocios Cisco AVVID. La administración de Pix ha sido también mejoradas a través de una fuerte integración con el cisco secure access control Server (ASC), permitiendo niveles de acceso administración, permitiendo recursos de la red y la estructuración de los servicios en grupos lógicos, para así tener políticas de control de acceso a la red.

PIX OS version 6.2 también se construye sobre la base de telefonía IP y servicios, multimedia entregados en la familia PIX firewall. Nuevas funcionalidades incluyen: servicios Porte address translation (PAT) para session iniative protol (SIP) y protocolos H 323.V2 y diversas opciones DHCP para comunicaciones con telefonias IP de Cisco y el softphone IP de Cisco. Stub Multicast Routing les permite a los clientes tomar ventajas de la muticast IP de banda ancha, a la vez que despliega aplicaciones multimedia como conferencias en video y aprendizaje. Ademas, entrega soporte para aplicaciones de Internet como Microsotf Netmeeking, que ha sido mejorada como apoyo al directorio de servicios locacion de Internet.

CONCLUSION

La conclusión de esta tesis es tener los conocimientos adecuados de los firewall, entender el concepto preciso de lo que es un firewall y saber cuál es la importancia.

Cuáles van hacer los niveles de filtración, como se va a trabajar en la capa de los firewall. La diversidad de los firewall, cuales son los tipos basado en su implementación.

Tipos de firewall: en la configuración de un firewall, la principal decisión consiste en elegir entre seguridad o facilidad de uso. Este tipo de decisiones es tomado en general por las direcciones de las compañías. Algunos firewall solo permiten tráfico de correos electrónicos a través de ellos, y por lo tanto protegen a la red contra cualquier ataque que no sea a través del servicio de correo. Otros son menos estrictos y solo bloquean aquellas servicios que se sabe que presentan problemas de seguridad.

Existen dos aproximaciones básicas:

- Todo lo que no es expresamente permitido está prohibido
- Todo lo que no es expresamente prohibido está permitido

Es un primer caso en firewall se diseña para bloquear todo el tráfico, y los distintos servicios deben ser activados de forma individual tras el análisis del riesgo que representan su activación y la necesidad de su uso. Esta política incide directamente sobre los usuarios de las comunicaciones, que pueden ver el firewall como un estorbo. En el segundo caso, el administrador del sistema debe que tipo de acciones pueden realizar los usuarios que pongan en entredicho la seguridad del sistema. Y preparar defensas contra ellas. Esta estrategia penaliza al administrador frente a los usuarios. Los puede comprometer inadvertidamente la seguridad del sistema si no conocen y cumplen unas consideraciones de seguridad mínima. El problema se magnifica si existen usuarios que tengan cuenta en la propia maquina que hace firewall (situación muy poco recomendable). En este tipo de estrategias hay un segundo peligro latente, y es que al administrador debe conocer todos los posibles agujeros existentes en los protocolos y las aplicaciones que estén corriendo los usuarios. El problema se agrava debido al hecho de que los fabricantes no suelen darse prisa en notificar los riesgos de seguridad que presenta sus productos.

Firewall a nivel de red

Por lo general se trata de un encaminador (router) o una computadora especial que examine la característica de los paquetes IP cuales deben pasar y cuáles no. Se podría configurar el encaminador para que se bloquee a todos los mensajes que provengan del sitio de un determinado al servidor de este competidor. Los profesionistas de redes a menudo denominan a este proceso lista negra

Las reglas de seguridad se definen para cada interfaz de red de firewall. Esto es así en los firewall es un enrutador que intenta hacer las funciones de firewall y de dispositivos de alta tecnología dedicada, como el firewall. Todos los paquetes se filtran basándose en las reglas que se aplican a la tarjeta de interfaz de red específica mediante la que se accedió al firewall. El hecho de configurar un firewall, entonces es en gran parte una cuestión de asignar reglas de seguridad a cada interfaz de firewall.

La lista de acceso es la herramienta más básica de seguridad de redes. La forma más sencilla de tecnología de seguridad de red es la lista de acceso. También llamadas lista de control de acceso a filtros, la lista de acceso es un componente básico de cualquier configuración de enrutador. Como el nombre indica, las listas de acceso restrieguen el tráfico al que se le permite acceder a una red. Las listas de acceso ofrecen un nivel básico de seguridad de red filtrado los paquetes e acuerdo tres criterios:

- **Dirección origen:** La dirección IP desee la que origino el paquete.
- **Dirección Destino:** La dirección IP (o direcciones) a la que se dirige el paquete.

- **Numero de puerto:** El protocolo del nivel aplicación (nivel 7) que usara el paquete.

La confiabilidad de los datos garantiza que únicamente las entidades con autorización **para ver los datos, los ven con formatos usables.**

GLOSARIO

Integridad: De los datos garantizan que los datos no han sido alterados ni destruidos por personan cuya consiste en modificarlos rotundamente.

Confidencialidad: De los datos garantiza que únicamente las entidades con autorización para ver los datos, los ven con su forma usable.

Direcciones IP: Se puede bloquear el acceso desde un IP específica, evitando ataques o consultas masivas a equipos servidores y clientes.

Nombre de Dominio: Consiste en tablas con nombres de computadoras vinculadas al DNS a donde no se permite el acceso de los usuarios locales.

Hurto de Información: Robo de información confidencial, tales como registros de clientes y empleados, o hurto de propiedad intelectual de su empresa.

Sabotaje de Información: Cambios a la información, en un intento de dañar la reputación de una persona o empresa. Como por ejemplo, elaborando o publicando contenido malintencionados en su sitio Web.

Negación de servicio (Dos, deniel of service): Bloqueo de los servidores o red de su empresa, de forma que los usuarios legítimos no puedan acceder a la información o, para impedir la operación normal de su empresa.

Hacker: Puede intentar obtener acceso a su red por diversión o ambición.

Servidor Proxy: Es un aplicación que actúa como intermediario entre dos sistemas finales. Los servidores Proxy funcionan en la capa de aplicación (nivel 7) de los firewall, donde se obliga a los extremos de una conexión a canalizar la sesión a través del Proxy.

PIX NAT: "Network address translation" trabaja sustituyendo, o traduciendo, direcciones de Host en la red interna con una "dirección global" asociada con una interfaz externa.

BIBILOGRAFIA

PAGINAS VISITADAS

http://www.dric.com.mx/seguridad/firewall2.php?cat=4

http://www.mulringles.net/docs/firewall.htm

http://www.terra.es/tecnoliga/articulo/html/tec10589.htm

http://www.segu-info.com.ar/firewall/firewall.htm

http://www.solocurso.net/firewall/firewall.htm

http://www.dabpweb.com7cas/tips/sto4-004-html

http://www.cisco.com/global/es/soltions/ent/avvid_solutions/vpn-home.shtml

http://wwwred-es.com/harware -software-conexion.htm

http://www.cisco.com/global/ES/indez.shtml

http://www.emagister.com/curso-firewall-kwes-358-htm

http://www.microsoft.com/spain/servidores/isaserver

LIBROS CONSULTADOS

HAYDEN Mat; Aprendiendo Redes en 24 horas

Prentice Hall, hispanoamericano, S.A

Pag.945

HILL Brian, Mc Graw; Cisco Manual de referencias tratamiento completo y actualizacion.

Diseño de seguridad de redes; Pearson educación S,A Madrid 20003

Diseño de Seguridad de redes; Pearson educación S.A Madrid 2003

ISBN84-205-3464-1.

“Seguridad Informatica”

Caballeros gil,pino, alfa omega

s/edición

INDICE DE LOS FIGURAS